CENTRAL ASIAN JOURNAL OF SOCIAL SCIENCES AND HISTORY

https://cajssh.centralasianstudies.org/index.php/CAJSSH

Volume: 05 Issue: 04 | July 2024 ISSN: 2660-6836

Article

Challenges and Implications of International Humanitarian Law in Cyberspace Warfare

Urmanova Madinahon Azizbek Kizi

Scientific article on competition for a doctorate degree philosophy in legal sciences (Doctor of Philosophy), Uzbekistan

* Correspondence: urmanovamadinahon12@gmail.com

Abstract: This study investigates the application of International Humanitarian Law (IHL) in the evolving landscape of cyberspace warfare, addressing the critical gap in existing legal frameworks regarding cyber operations. Utilizing a mixed-methods approach, including quantitative analysis of international protocols and agreements, the research identifies significant challenges in applying traditional IHL principles to cyber conflicts. The findings reveal inconsistencies in the regulation of cyber attacks, particularly in distinguishing between military and civilian targets and ensuring proportionality. The study concludes that current IHL principles are insufficient for the complexities of cyberspace, necessitating the development of new international norms and cooperation strategies. These results have significant implications for policymakers, highlighting the urgent need for updated legal frameworks to govern cyber warfare effectively.

Keywords: Cyber Technologies , IHL Principles, Nuclear Weapons, Civilian Object, Threat, Infrastructure.

1. Introduction

Information technology plays an important role in the modern world. They cover a wide range of technologies and systems that are used to process, store, transmit and analyze information, and the Internet is the basis of modern information technologies, providing access to a huge amount of information, online services, e-commerce and other opportunities[1]–[4]

International humanitarian law is applied in the context of armed conflicts to limit the use of force and protect non-combatants, such as civilians and medical personnel. However, in recent decades, with the development of cyber technologies, questions have arisen about how IHL applies in cyberspace[5]–[8].

In modern armed conflicts, cyber attacks pose a real threat. Disabling hospital computer systems, cutting off power to entire cities, poisoning water supplies. In cyberspace, IHL aims to protect civilians and humanitarian workers and limit the use of violence and destruction[9]–[12]. It also requires adherence to the principles of discrimination and proportionality in order to distinguish between military and civilian targets, limiting the use of force in accordance with the goals it seeks to achieve. However, due to the rapid development of technology and cyber threats , difficulties arise in applying traditional IHL rules to cyberspace[13]–[16]. Some issues, such as the definition

Citation: Urmanova Madinahon Azizbek Kizi. Challenges and Implications of International Humanitarian Law in Cyberspace Warfare. Central Asian Journal of Social Sciences and History 2024, 5(4), 147-153.

Received: 10th Apr 2024
Revised: 11th Mei 2024
Accepted: 24th Jun 2024
Published: 27th Jul 2024

of the boundary between peaceful and military activities in cyberspace, remain the subject of discussion and debate.

Critical life support services and basic infrastructure can be controlled via the Internet. But even wars have limits. The law of war limits the use of weapons, including cyber weapons. Civilians and civilian infrastructure must not be attacked. Malicious software that causes indiscriminate damage is prohibited. When conducting cyber operations during armed conflicts, international humanitarian law must be respected.

S.A. Gryaznov correctly noted , "cyberspace differs from ground, air, space and sea space, traditionally regulated by international law. Moreover, unlike conventional domains, cyberspace is a product of human creativity and not of so-called "natural" existence . " Moreover, the rapid development of digital technologies is dehumanizing armed conflicts. In an effort to limit the brutality of war, people created rules that also influenced the development and use of weapons. However, new technologies challenge existing legal norms.

There is general agreement in the international community that some principles of IHL can be applied to cyber warfare and cyber attacks, such as the distinction between military and civilian, proportionality, the prohibition of indiscriminate modes of warfare, the prohibition of indiscriminate modes of warfare, and the protection of critical infrastructure.

However, it is worth noting that issues related to cyber warfare and the application of IHL in cyberspace are still the subject of debate in international law. In recent years, international organizations and countries have been working to develop norms and regulations that could set standards of conduct in cyberspace and incorporate aspects of IHL.

2. Materials and Methods

This study uses a mixed methods approach involving quantitative analysis of the characteristics of international community protocols and agreements. When analyzing data, a standardized rubric is used to assess the level of development of military information technologies, which allows us to talk about a new theater of military operations - information space (cyberspace). The likelihood of an armed conflict in cyberspace is also confirmed by the Tallinn Manual on International Law Applicable to Cyber Operations , developed in 2013 and updated in 2017 by specialists from the countries of the military-political NATO bloc with the participation of the International Committee of the Red Cross .

What we call artificial intelligence , or more precisely neural networks, is a certain algorithm that has the ability to obtain a huge amount of information. In each piece of information, some of its own aspects are highlighted, which are different information on which artificial intelligence and the neural network should pay attention and by analyzing this entire sequence of data, it can assume a greater or lesser probability that the newly arriving data is a long topic.

3. Results and Discussion

Rules of war (rules of international humanitarian law). These universal rules of war establish basic restrictions on the methods and means of warfare so that they protect those who do not participate in hostilities, as well as those who can no longer take part in them.

To do this, a distinction must always be made between those persons and objects that can be attacked and those that must be spared and protected. The most important rule is to prevent attacks on civilians. Such actions are war crimes. Every possible measure must be taken to prevent harm to civilians and the destruction of facilities essential to their survival. These persons have the right to receive all necessary assistance.

Technical progress in the field of weapons requires that appropriate changes be made to the rules of the law of war when using certain types of weapons and methods of warfare. No distinction is made between persons participating in hostilities and civilian violence . Therefore, agreements were reached on restrictions on the use of such types of weapons and methods of warfare.

The meaning of international humanitarian law is to preserve and preserve, as far as possible, human dignity in times of war and so that people can reconcile with each other after the last shot is fired.

Cyberspace is a term that describes the virtual space created by computer systems and networks where information is exchanged, stored and processed. This includes the Internet, computer networks, databases and other digital systems. In today's world, cyberspace is of great importance in various fields, including economics, politics, education and military operations.

In the context of modern military conflicts, cyberspace has become an important factor that influences military strategies, tactics and operations.

This is why cyberspace is so important in modern military conflicts.

Cyberspace is used to perform the following actions:

- Cyberattacks: States and non-state actors can use cyberattacks to invade the computer systems of other countries, steal confidential information, destroy critical infrastructure, etc.
- Espionage: Cyberspace provides the opportunity for large-scale espionage, including intelligence gathering about military strategies and operations.
- Electronic warfare: Military forces can use cyberspace to conduct electronic warfare, including jamming enemy communications and radar systems.
- Manipulation of information and disinformation : Cyberspace allows for the spread of disinformation and the manipulation of public opinion, which can have an important impact on the course of military conflicts.
- Cybersecurity : Ensuring security in cyberspace has become a key aspect of protecting national security. States must protect their computer systems from cyber attacks and other threats.
- Cyber weapons : There are military programs developing cyber weapons that can damage enemy computer systems.

All these aspects highlight the importance of cyberspace in modern military conflicts and the need to develop effective strategies to protect against cyber threats and use cyberspace in military operations. International Humanitarian Law (IHL) is an important area of international law that establishes rules and principles for the protection of non-combatants and limits the conduct of war. It regulates the behavior of conflicting parties during armed conflicts and aims to reduce suffering associated with wars and conflicts.

These IHL principles provide the basis for the ethical conduct of war and aim to reduce suffering and protect the fundamental rights and dignity of people in times of armed conflict.

International Humanitarian Law (IHL) is a set of rules and principles designed to protect non-combatants and limit the conduct of war. In the context of cyber attacks, these principles can be applied as follows:

1. The principle of inadmissibility of arbitrary violence and inhuman treatment. This principle means that cyber attacks should not cause excessive harm to civilian objects or civilians. Cyberattacks cannot be directed at targets that are not involved in military operations, such as medical facilities or civilian servers.
2. The principle of the necessity of distinction. This principle requires a distinction between military and civilian targets. Cyber attacks should only be directed at military targets and should not harm civilian facilities such as critical infrastructure (energy systems, water supplies, transport networks) unless they are used for military purposes.
3. Principle of Proportionality. Cyber attacks should not be excessively proportionate to the military benefit they bring. That is, the level of damage caused by a cyber attack should not exceed the expected military benefit that it brings to the attacking party.
4. The principle of prohibition of sophisticated methods of struggle. This principle prohibits the use of cyberattacks that are likely to cause unnecessary suffering or fail to distinguish between military and civilian targets. For example, cyberattacks targeting medical systems or transportation network management systems could endanger civilian lives and violate this principle.
5. Principle of Protection of persons not participating in hostilities. This principle requires that civilians and installations, such as medical facilities and humanitarian organizations, not be attacked. Cyberattacks cannot be directed at systems providing humanitarian aid or medical assistance.

The application of these principles in the context of cyberattacks highlights the importance of developing international norms and standards to govern cyber warfare and the protection of civilians and assets in cyberspace.

Practical results

Advances in technology play a key role in the evolution of cyber attacks and create new opportunities for hackers and cybercriminals. Here are some aspects of technological development that influence cyber attacks:

- Automate cyberattacks: Artificial intelligence and machine learning algorithms can be used to automate hacking processes, speeding up cyberattacks and the discovery of security vulnerabilities.
- Phishing and Social Engineering: Machine learning algorithms can help create more convincing phishing emails and disguise them, making them more difficult for users and security systems to detect.
- Cryptography : The development of quantum computing could undermine current cryptography techniques used to protect data online, opening up new vulnerabilities and attack surfaces.
- Botnets and DDoS attacks : IoT devices such as smart homes and industrial devices can be hijacked into botnets and used for large-scale DDoS attacks targeting organizations and servers.
- Quantum cryptography: The development of quantum cryptography can lead to the creation of secure communication channels that cannot be attacked by classical cryptography methods.

- Blockchain technology : Blockchain can provide secure and anonymous transactions, which can be used for cybercrimes such as extortion using cryptocurrencies.

All of these technology trends create new cybersecurity challenges. Information security defenders must stay abreast of these trends and actively develop new methods of detecting and defending against cyberattacks to combat the ever-changing threats in cyberspace.

Challenges and Problems in Cyberspace.

The application of international humanitarian law (IHL) in cyberspace faces a number of complexities and challenges, mainly due to the technical nature of cyber attacks and the rapid development of cyber technologies .

Some of them are listed below:

1. Difficulty in identifying attackers : In cyberspace, it is difficult to accurately identify and attribute cyber attacks to specific countries or actors , due to the use of anonymous technical methods and proxy servers.
2. Unclear definitions: The definition of cyberattacks and their classification as military or civil acts can be controversial and cause disagreement among states and experts.
3. Difficulties in determining proportionality: Unlike physical attacks, determining proportionality in cyber attacks, especially in the case of non-military actors , is a difficult task.
4. Cyber attacks on civilian objects. Cyberattacks on civilian assets, such as medical facilities and energy systems, can cause excessive suffering and loss of life, but are difficult to accurately identify and protect.
5. Collective responsibility : In the event that a cyber attack is carried out on behalf of non-state actors , it is difficult to establish state responsibility for these actions, which makes enforcement under IHL difficult.
6. Protecting Humanitarian Data: Cyberattacks can include the theft or destruction of humanitarian data such as medical records, highlighting the need to protect sensitive humanitarian information.

Addressing these challenges requires concerted efforts among States and international organizations to develop clear rules and regulations governing how IHL applies in cyberspace, as well as assistance in cybersecurity and improved technical means for attributing cyber attacks.

It also highlights the importance of constantly updating laws and standards in line with evolving cyber technologies and threats in cyberspace.

4. Conclusion

Improving the application of international humanitarian law (IHL) in cyberspace requires joint efforts by international communities, states and technical experts. Here are some recommendations and possible solutions to improve compliance with IHL in the context of cyber warfare:

1. Promotion of international agreements: Encourage states to develop and adopt international norms and agreements that would define rules and standards for cyber warfare and emphasize their compliance with existing principles of IHL.
2. Development of international cooperation and dialogue: Encouraging international dialogue and cooperation between states to exchange information on cyber threats and develop joint cybersecurity strategies.

3. Development of technical means of attribution: Investments in research and development of technical methods for attribution of cyber attacks, which will allow more accurately identifying the sources of attacks.
4. Improving Transparency of Operations: States must be more transparent about their cyber operations , especially those that may have a military impact.
5. Education and Knowledge Outreach: Increase efforts in cyber education and disseminate cybersecurity best practices to ensure a thorough understanding of IHL and cyber threats .

Conducting global campaigns to disseminate information about the importance of respect for IHL in cyberspace and the consequences of violating it.Development of humanitarian cyber defense : Development and implementation of specialized security measures for humanitarian organizations, medical institutions and other sites providing humanitarian assistance in the event of conflict.

Creation of international expert groups: Formation of international organizations or expert groups to study and develop recommendations for the application of IHL in cyberspace.Solving these problems will require much effort and concerted action between states, international organizations, civil society and the private sector. Only through international cooperation and adherence to the principles of IHL can sustainable and ethical development of cyberspace be achieved.

As you probably want to ask, can cyber operations trigger armed conflict, it would be reasonable to say that they can. But if you look at the conditions that determine the outbreak of a traditional armed conflict, they consist of the use of force by organized armed groups. That is, if there are organized military forces that systematically use cyber operations to inflict damage on, for example, a state, this is likely to start an armed conflict. But in practice , governments have yet to confirm this.

REFERENCES

[1] A. Khalil, "NAVIGATING LEGAL FRONTIERS IN CYBER WARFARE: INSIGHTS FROM THE RUSSIA-UKRAINE CONFLICT," *Lawyer Q.*, vol. 14, no. 2, pp. 252–267, 2024.

[2] D. J. B. Svantesson, "Regulating a 'Cyber Militia' – Some Lessons from Ukraine, and Thoughts about the Future," *Scand. J. Mil. Stud.*, vol. 6, no. 1, pp. 86–101, 2023, doi: 10.31374/sjms.195.

[3] E. Oğurlu, "International Law in Cyberspace: An Evaluation of the Tallinn Manuals," *Ann. la Fac. Droit d'Istanbul*, no. 73, pp. 327–344, 2023, doi: 10.26650/annales.2023.73.0010.

[4] M. Watin-Augouard, "The boundary between cybercrime and cyberwar: An uncertain no-man's land," *Conflicts, Crimes Regul. Cybersp.*, pp. 89–105, 2021, doi: 10.1002/9781119885092.ch4.

[5] B. Pratama, "Tallinn manual: Cyber warfare in Indonesian regulation," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 729, no. 1, 2021, doi: 10.1088/1755-1315/729/1/012033.

[6] Z. Huang, "The application of the principle of distinction in the cyber context: A Chinese perspective," *Int. Rev. Red Cross*, vol. 102, no. 913, pp. 335–365, 2020, doi: 10.1017/S1816383121000023.

[7] M. A. Khan, "Reducing the Threat of Cyber Warfare Through a Suitable Dispute Resolution Mechanism," *Law J. Univ. Latv.*, vol. 2020, no. 13, pp. 97–120, 2020, doi: 10.22364/jull.13.06.

[8] G. D. Brown, "International law and cyber conflict," *Routledge Handb. Int. Cybersecurity*, pp. 366–378, 2020, doi: 10.4324/9781351038904-36.

[9] J. Beard, "The principle of proportionality in an era of high technology," *Complex Battlespaces Law Armed Confl. Dyn. Mod. Warf.*, vol. 1, pp. 261–288, 2018, doi: 10.1093/oso/9780190915360.003.0009.

[10] M. N. Schmitt, "Complex battlespaces: The law of armed conflict and the dynamics of modern warfare," *Complex Battlespaces Law Armed Confl. Dyn. Mod. Warf.*, vol. 1, pp. 1–528, 2018, doi: 10.1093/oso/9780190915360.001.0001.

[11] P. Mali, "Cyber-terrorism as a non-state cyber warfare: An overview," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 2, pp. 859–872, 2018.

[12] H. P. Faga, "The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century," *Balt. J. Law Polit.*, vol. 10, no. 1, pp. 1–34, 2017, doi: 10.1515/bjlp-2017-0001.

[13] K. Kittichaisaree, "Application of the Law of Armed Conflict, Including International Humanitarian Law, In Cyberspace," *Law, Gov. Technol. Ser.*, vol. 32, pp. 201–231, 2017, doi: 10.1007/978-3-319-54657-5_5.

[14] C. Trezza, "Negotiation on cyber warfare," *Adv. Sci. Technol. Secur. Appl.*, pp. 257–264, 2017, doi: 10.1007/978-3-319-54975-0_16.

[15] J. Domínguez-Bascoy, "War-like activities in the cyberspace: Applicability of the law of armed conflicts," *Adv. Sci. Technol. Secur. Appl.*, pp. 243–256, 2017, doi: 10.1007/978-3-319-54975-0_15.

[16] D. Garcia, "Future arms, technologies, and international law: Preventive security governance," *Eur. J. Int. Secur.*, vol. 1, no. 1, pp. 94–111, 2016, doi: 10.1017/eis.2015.7.

[17] Kommersant US intelligence agencies have confirmed a large-scale cyber attack on the government. – [Electronic resource]. – Access mode: https://www.kommersant.ru/doc/4616730 (access date: 01/16/2021)

[18] Danelyan A.A. International legal regulation of cyberspace. – [Electronic resource]. – Access mode: https://cyberleninka.ru/article/n/mezhdunarodno-pravovoeregulirovanie-kiberprostranstva (date of access: 01/16/2021)

[19] D- Russia The Russian Foreign Minister called for the development of a universal international code of conduct in cyberspace. – [Electronic resource]. – Access mode: https://www.iksmedia.ru/news/5694541-Glava-MID-RF-prizval-vyrabotat-univ.html (access date: 01/16/2021)

[20] Kovacic L. The Chinese example is contagious. – [Electronic resource]. – Access mode: https://www.vedomosti.ru/opinion/articles/2019/01/28/792659-primer (access date: 01/16/2021)

[21] Lankov A. Is there Internet in the DPRK and who can use it? – [Electronic resource]. – Access mode: https://profile.ru/abroad/chtoby-ne-dopustit-kramoly-vsevernoj-koree-sozdali-svoyu-sistemu-interneta-251402/ (access date: 01/16/2021)