THE POTENTIAL HUMAN COST OF CYBER OPERATIONS

Vareena Rizvi & Priyanka Srivastava, Amity University, Lucknow

ABSTRACT

Cyber operations have become an increasingly important aspect of modern conflicts. The potential human cost of cyber operations is a complex and multifaceted issue that has become increasingly relevant in modern conflicts. Cyber operations can cause direct harm to civilians and civilian objects, as well as indirect harm and economic harm. The application of International Humanitarian Law (IHL) to cyber operations presents challenges, particularly in predicting the effects of cyber-attacks and responding to them. This paper explores the potential humanitarian impact of cyber operations, including direct and indirect harm to civilians, as well as economic harm. It also discusses the challenges associated with applying international humanitarian law (IHL) to cyber operations, particularly with regard to the principles of distinction and proportionality. Additionally, the paper discusses the applicability of other legal frameworks to cyber operations, such as human rights law and the law on state responsibility. Finally, the paper identifies areas for further research and discusses the implications of cyber operations for future conflicts.

INTRODUCTION

Cyber operations refer to the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[1] They are activities conducted in cyberspace by individuals, groups, or states using technology to achieve specific objectives. These objectives may include espionage, sabotage, theft, disruption, or destruction of computer systems, networks, and data. Cyber operations may involve various techniques such as hacking, malware deployment, social engineering, and phishing. They may be conducted for various purposes, including military, political, economic, or criminal motives, and are often complex and sophisticated, involving multiple stages and actors, and can have significant consequences for individuals, organizations, and governments.

Cyber operations have emerged as a crucial element in modern conflicts due to the increasing dependence on technology in various aspects of life, including military operations. Cyberattacks are considerably different from traditional 'kinetic' warfare: they do not involve direct force, do not (yet) destroy in the conventional sense of the word, and are difficult to attribute to specific actors.[2] They offer a low-cost, high-impact means of achieving military objectives, particularly in situations where the use of force is constrained by international law or political considerations. They can disrupt critical infrastructure, communications systems, and weapons systems, providing a strategic advantage to the attacker. Moreover, cyber operations are difficult to attribute to a specific actor, making it harder for states to hold the attacker accountable. This has lowered the threshold for initiating cyber operations, particularly among non-state actors. Thus, the importance of cyber operations in modern conflicts cannot be overstated.

The applicability of International Humanitarian Law (IHL)[3] to cyber operations is an

[1] CSRC Content Editor *cyberspace operations (CO) - Glossary | CSRC*. Available at: https://csrc.nist.gov/glossary/term/cyberspace_operations.
[2] Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," Foreign Affairs, Nov/Dec. 2013.
[3] International humanitarian law (IHL) is a set of rules that aim to limit the effects of armed conflicts on civilians and combatants. It includes the Geneva Conventions and their Additional Protocols, as well as customary international law.

ongoing debate. Some argue that existing IHL rules on targeting, proportionality, and distinction can be applied to cyber operations, while others argue that new rules are needed to address the unique characteristics of cyberspace. In general, IHL applies to cyber operations that have a nexus to an armed conflict, including those conducted as part of a military operation or those that have a direct or indirect impact on the conduct of hostilities.

IHL rules on targeting require that attacks be directed only at military objectives and that any expected harm to civilians or civilian objects be proportionate to the expected military advantage gained. The principle of distinction requires parties to the conflict to distinguish between civilians and combatants, and between civilian objects and military objectives. These rules apply to cyber operations in the same way as they do to traditional military operations.

However, cyber operations add a new level of complexity to armed conflict that may pose novel questions for IHL. As a result, IHL's relevance needs to be reaffirmed as the principal body of law that can regulate such warfare. The norms in international humanitarian law covering such issues as the use of indiscriminate weapons, the distinction between military targets and civilians, proportionality, and perfidy, can and must be applied also to cyber warfare.[4]

IHL applies to all types of armed conflicts, whether international or non-international, and to all parties involved in such conflicts, including states and non-state actors.

[4] International Committee of the Red Cross (2010) "Cyber warfare," *International Committee of the Red Cross*, 29 October. Available at: https://www.icrc.org/en/document/cyber-warfare.

POTENTIAL HUMAN COST OF CYBER OPERATIONS

The use of cyber operations may present alternatives to other forms of warfare, but it also carries risks. On the one hand, cyber operations have the potential to allow parties to armed conflicts to achieve their military objectives without harming civilians or causing physical damage to civilian infrastructure. On the other hand, recent cyber operations, the majority of which were carried out outside of an armed conflict, demonstrate that knowledgeable actors have gained the ability to obstruct the delivery of vital services to the civilian population (International Committee of the Red Cross, 2010).[5]

The potential human costs of cyber operations under international humanitarian law (IHL) are significant, as cyber-attacks can have severe and lasting consequences on civilians, combatants, and critical infrastructure. Cyber attacks can cause physical harm, such as the destruction of buildings or vehicles, or the disabling of medical devices or transportation systems. They can also disrupt essential services such as water and electricity, which can have severe consequences for public health and safety.

Moreover, the effects of cyber attacks can be long-lasting, as it may take significant time and resources to restore affected systems or infrastructure. In addition, cyber attacks can have psychological impacts on individuals and communities, as they may cause fear, anxiety, and trauma.

Cyber operations must be conducted with due regard for the principles of distinction, proportionality, and military necessity, and attacks must only be directed at military objectives. Under IHL, parties to a conflict must take all reasonably practicable measures to avoid or minimize harm to civilians and civilian objects, and must refrain from attacks that would cause excessive harm to the civilian population (International Committee of the Red Cross, 2019).

However, the nature of cyberspace presents challenges in complying with these

[5] See ICRC, The Potential Human Cost of Cyber Operations, 2019; available at https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

principles, as it can be difficult to determine the specific target of a cyber attack and assess its potential impact on civilians and civilian objects. Moreover, the attribution of cyber attacks can be difficult, which can make it challenging to hold responsible parties accountable for any harm caused.

The potential human cost of cyber operations under international humanitarian law (IHL) can take several forms, including direct harm to civilians and civilian objects, indirect harm to civilians, and economic harm to civilians and civilian objects.[6]

Direct harm to civilians and civilian objects can occur when cyber attacks result in the destruction or disabling of critical infrastructure, such as hospitals, water treatment plants, or power grids. Additionally, cyber attacks can cause harm to civilians by disrupting essential services, such as transportation systems or emergency communication networks.

Indirect harm to civilians can occur as a result of the consequences of cyber attacks, such as the loss of critical data or disruption of essential services. For example, a cyber attack on a hospital's computer system could result in the loss of patient records, leading to delays in medical treatment and potentially harming patients' health.

Economic harm to civilians and civilian objects can occur when cyber attacks disrupt businesses, financial systems, and critical infrastructure. For example, a cyber attack on a financial institution could result in the loss of sensitive financial information or the disruption of banking services, which could have a significant impact on individuals and businesses that rely on these services. Similarly, a cyber attack on a power grid or transportation system could disrupt economic activity and cause widespread economic harm.

Parties to a conflict must take into account the potential economic repercussions of cyber operations and take steps to minimize harm to the civilian population under International Humanitarian Law (IHL), which requires parties to refrain from attacks that would cause

[6] see, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts* (2021). Available at: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913.

excessive harm to the civilian population (International Committee of the Red Cross, 2019).

However, the nature of cyberspace presents challenges in complying with these principles, as it can be difficult to predict the potential economic consequences of a cyber attack. Moreover, the attribution of cyber attacks can be difficult, which can make it challenging to hold responsible parties accountable for any economic harm caused. A cyber attack on a specific system may have repercussions on various other systems, regardless of where those systems are located. There is a real risk that cyber tools – either deliberately or by mistake – may cause large-scale and diverse effects on critical civilian infrastructure. The interconnectedness of cyberspace also means that all States should be concerned with its effective regulation: "Attacks carried out against one State can affect many others – wherever they are located and irrespective of whether they are involved in the conflict".[7]

Under IHL, parties to a conflict must take all feasible precautions to avoid or minimize harm to civilians and civilian objects and must refrain from attacks that would cause excessive harm to the civilian population. This means that parties to a conflict must consider the potential consequences of cyber operations and take steps to minimize harm to the civilian population. The nature of cyberspace, however, makes it difficult to uphold these principles because it can be challenging to foresee potential outcomes of a cyberattack and assign blame for any damage that results (Rushing, 2021).

To address the particular difficulties in applying IHL to cyber operations and to guarantee that cyber operations adhere to the principles of IHL in the context of contemporary conflicts, more legal and policy development is required.

[7] Helen Durham, "Cyber Operations during Armed Conflict: 7 Essential Law and Policy Questions", Humanitarian Law and Policy Blog, 26 March 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions.

INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS

International humanitarian law (IHL) applies to all forms of armed conflict, including those that involve cyber operations. IHL seeks to limit the effects of armed conflict by regulating the conduct of hostilities and protecting civilians and civilian objects from harm. In the context of cyber operations, IHL imposes obligations on parties to the conflict to minimize harm to civilians and civilian objects, and to ensure that cyber operations are conducted in compliance with the principles of distinction, proportionality, and precaution.

THE PRINCIPLES OF PROPORTIONALITY AND DISTINCTION

The principles of proportionality and distinction are two of the fundamental principles of international humanitarian law (IHL) that apply to all forms of armed conflict, including cyber operations.

The principle of proportionality prohibits attacks against military objectives which are "expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[8] This means that parties must assess the expected harm caused by an attack, including the incidental loss of civilian life or damage to civilian objects, and weigh it against the expected military advantage. If the expected harm to civilians or civilian objects outweighs the expected military advantage, the attack is prohibited.

The principle of distinction is a fundamental principle of international humanitarian law which provides that parties to an armed conflict must "at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military

[8] *Proportionality | How does law protect in war? - Online casebook* (no date). Available at: https://casebook.icrc.org/a_to_z/glossary/proportionality.

objectives".[9] This means that attacks must be directed only at military objectives and cannot be directed at civilians or civilian objects. Parties must take all feasible precautions to ensure that their attacks are limited to military objectives and do not cause harm to civilians or civilian objects. The principle of distinction also requires parties to take all feasible precautions to verify that the target is a military objective before attacking.

Both principles are crucial in the context of cyber operations. Cyber attacks must be directed at military objectives and must not cause harm to civilians or civilian objects. Parties to a conflict must take all feasible precautions to ensure that their cyber operations do not harm civilians or civilian objects. Furthermore, parties must assess the potential consequences of their cyber operations and weigh them against the expected military advantage to ensure that their operations comply with the principle of proportionality.

The application of these principles to cyber operations can be complex and challenging, given the unique characteristics of cyberspace. For example, it can be difficult to distinguish between military and civilian targets in cyberspace, and the potential harm caused by cyber operations can be difficult to predict. However, parties to a conflict must take all feasible measures to comply with these principles and to minimize harm to civilians and civilian objects.

APPLICABILITY OF IHL TO CYBER OPERATIONS

The applicability of International Humanitarian Law (IHL) to cyber operations is a complex and evolving area of international law. However, it is clear that IHL applies to cyber operations that occur in the context of an armed conflict, whether international or non-international in character. When States adopt IHL treaties, they do so to regulate present and future conflicts. States have included rules that anticipate the development of new means and methods of warfare in IHL treaties, presuming that IHL will apply to them. For instance, if IHL did not apply to future means and methods of warfare, it would not be necessary to review their lawfulness under existing IHL, as required by

[9] *Distinction | How does law protect in war? - Online casebook* (no date). Available at: https://casebook.icrc.org/a_to_z/glossary/distinction.

Article 36 of the 1977 First Additional Protocol.[10]

The definition of armed conflict in IHL is broad and includes both international and non-international armed conflicts. A cyber operation can constitute an armed attack and trigger the application of IHL if it reaches a certain threshold of intensity and violence, causes damage or destruction of civilian objects, or results in death or injury to persons. This means that IHL applies to cyber operations that occur in the context of an armed conflict, regardless of whether the cyber operations themselves are considered an act of war. The ICRC understands "cyber operations during armed conflict" to mean operations against a computer system or network, or another connected device, through a data stream, when used as a means or method of warfare in the context of an armed conflict.[11]

IHL imposes obligations on parties to an armed conflict to minimize harm to civilians and civilian objects, and to ensure that their cyber operations are conducted in compliance with the principles of distinction, proportionality, and precaution. These principles require parties to distinguish between military objectives and civilians and civilian objects, to weigh the expected military advantage of a cyber operation against the harm it may cause to civilians and civilian objects, and to take all feasible precautions to minimize harm to civilians and civilian objects.

CHALLENGES IN APPLYING IHL TO CYBER OPERATIONS

Applying International Humanitarian Law (IHL) to cyber operations poses a number of challenges. The unique characteristics of cyberspace make it difficult to determine who is responsible for a cyber operation, classify it as either international or non-international armed conflict, distinguish between military and civilian targets, predict the effects of cyber operations, respond to cyber attacks, and create a consensus on the applicability

[10] International Committee of the Red Cross (2019b) "International humanitarian law and cyber operations during armed conflicts," *International Committee of the Red Cross*, 28 November. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

[11] International Committee of Red Cross (2011), *International humanitarian law and the challenges of contemporary armed conflicts*, *icrc.org*. 31IC/11/5.1.2. 31st INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT Geneva, Switzerland 28 November – 1 December 2011. Available at: https://www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf.

of IHL to cyber operations. Addressing these challenges requires continued engagement and dialogue among states, international organizations, and other stakeholders to ensure that the legal framework governing cyber operations is clear, effective, and able to keep pace with technological developments.

One of the key challenges is the difficulty in attributing a cyber operation to a specific actor or state. Cyber attacks can be launched from anywhere in the world, and the use of proxies and other obfuscation techniques can make it difficult to identify the true source of an attack. This creates challenges for applying IHL's principles of distinction and proportionality, which require that attacks be directed only at military objectives and that any harm to civilians or civilian objects be proportionate to the military advantage gained.[12]

Another challenge is the classification of cyber operations as either international or non-international armed conflicts. Cyber operations can be launched by non-state actors, such as hacktivist groups or criminal organizations, or can take place outside the territory of a state, making it difficult to determine whether they meet the criteria for an armed conflict.

In addition, distinguishing between military and civilian targets in cyberspace can be challenging. Many civilian objects, such as critical infrastructure, can also have military significance, which can make it difficult to determine whether an attack on such objects is permissible under IHL.

The challenges associated with cyber operations under international humanitarian law are not limited to the conduct of such operations but also extend to their potential impact and response. Predicting the potential effects of a cyber attack can be challenging, as the impact can be highly unpredictable and can quickly spread beyond its intended target. This can make it difficult to assess the potential harm to civilians and civilian objects, as well as to determine the proportionality of an attack. Additionally, responding to cyber attacks can be problematic due to the lack of clear rules governing

[12] see, Iberdrola (2021) "Cyber Warfare in context of global conflicts," *Iberdrola* [Preprint]. Available at: https://www.iberdrola.com/shapes-en/keren-elazari-cyber-warfare-in-context-of-global-conflicts.

countermeasures and the difficulty in identifying the origin of an attack. This can make it difficult for states to respond in a manner that is consistent with IHL.

Finally, there is an ongoing debate and a lack of consensus among states and other stakeholders on the applicability of IHL to cyber operations. This creates uncertainty in the legal framework governing cyber operations and can make it difficult for states to know how to respond to cyber attacks in a manner that is consistent with IHL.

Overall, addressing these challenges requires continued engagement and dialogue among states, international organizations, and other stakeholders to ensure that the legal framework governing cyber operations is clear, effective, and able to keep pace with technological developments.

COMPLIANCE WITH OTHER LEGAL FRAMEWORKS

HUMAN RIGHTS LAW

International human rights law (IHRL) is a legal framework that sets out the rights and freedoms that are guaranteed to individuals under international law. It applies to all states and is grounded in the principles of dignity, equality, and non-discrimination. Human rights law is applicable to cyber operations that have an impact on the human rights of individuals, such as the right to privacy, freedom of expression, and freedom of assembly.

In the context of cyber operations, human rights law requires states to ensure that their actions do not violate fundamental human rights. For example, states must ensure that their cyber operations do not result in arbitrary or unlawful surveillance or censorship and that individuals are not targeted for their political beliefs, religion, or other protected characteristics.[13]

Human rights law also requires states to provide effective remedies for individuals who have been harmed by cyber operations. This may include providing access to justice, compensation for damages, and other forms of redress.

Overall, compliance with international human rights law is essential to ensuring that cyber operations are conducted in a manner that respects the rights and freedoms of individuals. By considering the human rights implications of their actions, states and other actors can help to promote a secure and stable cyberspace that protects the dignity and rights of all individuals.

LAW ON STATE RESPONSIBILITY

The law on state responsibility is a legal framework that governs the responsibility of states for their actions under international law. It provides a framework for determining when states are responsible for violations of international law, including violations

[13] This essay will be more concerned with another aspect, namely the right to privacy, protected under Article 12 of the UDHR and Article 17 of the ICCPR. Article 17 of the ICCPR provides: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

related to cyber operations.

Under the law on state responsibility, states are responsible for any act or omission that is attributable to the state and that constitutes a breach of an international legal obligation. This includes obligations under international humanitarian law, human rights law, and other legal frameworks.

In the context of cyber operations, states may be held responsible for actions that violate international law, including those that result in harm to civilians or civilian objects. For example, a state may be responsible for cyber operations that result in the destruction of critical infrastructure or that cause harm to civilians. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.[14]

When a state is found to be responsible for a violation of international law, it may be required to provide remedies, such as compensation or restitution, to the affected individuals or states. In some cases, state responsibility may also lead to diplomatic or economic consequences, such as the imposition of sanctions or other penalties.

Overall, the law on state responsibility is an important legal framework for ensuring that states are held accountable for their actions under international law, including those related to cyber operations. By complying with their international legal obligations, states can help to promote stability, security, and the rule of law in cyberspace.

DOMESTIC LAW

Domestic law refers to the laws and regulations of a particular country or jurisdiction. In the context of cyber operations, domestic law may include a range of legal frameworks and regulations, such as those related to data protection, cybercrime, national security, and intellectual property.

[14] UN GGE 2015 report (n 46) 8, norm (f). Secretary-General, Un. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :: note /: by the Secretary-General*. Available at: https://digitallibrary.un.org/record/799853?ln=en.

Domestic laws and regulations related to data protection may be particularly relevant in the context of cyber operations. These laws may establish requirements for the collection, use, and storage of personal data, as well as provide remedies for individuals whose data has been breached or otherwise misused. Compliance with data protection laws may be particularly important in the context of cyber operations that involve the collection or transmission of sensitive personal information.

Cybercrime laws are another important aspect of domestic law related to cyber operations. These laws may establish criminal offenses related to unauthorized access to computer systems, theft of data, and other forms of cybercrime. Compliance with cybercrime laws may be particularly important in the context of cyber operations that involve hacking or other unauthorized access to computer systems. The vast majority of cyberattacks fall on small, private enterprises, not on government infrastructure. This reality requires civil and domestic responses, rather than military ones.[15]

National security laws and regulations may also be relevant in the context of cyber operations. These laws may establish requirements for the protection of national security interests, such as the protection of critical infrastructure or sensitive government information. Compliance with national security laws may be particularly important in the context of cyber operations that involve attacks on government systems or other sensitive targets.

Overall, domestic law plays an important role in regulating and controlling activities related to cyber operations. Compliance with domestic laws and regulations is essential for ensuring that cyber operations are conducted in a lawful and responsible manner. States and other actors should be aware of the domestic legal frameworks that apply in their respective jurisdictions and take steps to ensure compliance with applicable laws and regulations.

[15] Justin Malzac "Leveraging Domestic Law Against Cyberattacks," American University National Security Law Brief, Vol. 11, No. 1 (2021). Available at: https://digitalcommons.wcl.american.edu/nslb/vol11/iss1/2

CONCLUSION

In conclusion, cyber operations have become an increasingly important aspect of modern conflicts. As such, it is crucial to ensure that these operations are conducted in a manner that is consistent with international humanitarian law (IHL) and other relevant legal frameworks. This includes adhering to the principles of proportionality and distinction, taking precautions to minimize harm to civilians and civilian objects, and providing assistance to affected civilians. However, applying IHL to cyber operations presents several challenges, including issues related to attribution, the identification of military objectives, and the assessment of potential humanitarian impact. To address these challenges, it is important to take a comprehensive approach that includes measures to avoid or minimize harm, as well as assistance to affected civilians. Moreover, it is essential to ensure compliance with domestic laws and regulations, including those related to data protection, cybercrime, and national security. By adopting a proactive and responsible approach to cyber operations, states and other actors can help to ensure that these operations are conducted in a manner that respects the rights and well-being of all individuals affected by them.

Cyber operations should not be thought of as a computer against a computer but as a much broader concept. It is an effort through cyberspace or using digital means to attack an opponent.[16]

The implications of the potential humanitarian cost of cyber operations under international humanitarian law for future conflicts are significant. As cyber operations continue to be an increasingly important aspect of modern conflicts, there is a growing need for greater awareness of the potential humanitarian impact of these operations. States and other actors must be aware of their legal obligations under IHL and take proactive measures to ensure that cyber operations are conducted in a manner that

[16] *Cyber Warfare: The New Front | George W. Bush Presidential Center* (2022). Available at: https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.

respects these obligations.

Furthermore, as technology continues to advance and cyber operations become more sophisticated, the challenges of applying IHL to these operations will likely become more complex. States and other actors will need to remain vigilant and adaptive in order to ensure that IHL remains relevant and effective in regulating the conduct of armed conflicts, including those that involve cyber operations.

Overall, the potential humanitarian cost of cyber operations highlights the importance of a comprehensive and responsible approach to conducting cyber operations in future conflicts. By prioritizing the protection of civilians and civilian objects, and by taking proactive measures to minimize harm and provide assistance to affected individuals, states and other actors can help to ensure that the impact of cyber operations on civilians is minimized and that these operations are conducted in a lawful and responsible manner.

There are several areas that require further research regarding the potential humanitarian impact of cyber operations under international humanitarian law.[17] Firstly, new technologies are continuously emerging and it is important to assess their impact on the conduct of cyber operations in armed conflicts, and ensure they are subject to the appropriate legal and regulatory frameworks. Secondly, as non-state actors increasingly participate in cyber operations, it is important to determine their legal obligations under IHL and ensure they are held accountable for any violations. Thirdly, attributing cyber operations to specific actors is becoming more difficult, and it is necessary to investigate the implications of this for compliance with IHL and the accountability of actors for violations. Finally, research should examine the role of international organizations and the international community in regulating the conduct of cyber operations in armed conflicts to ensure they are consistent with international legal obligations and promote the protection of civilians and civilian objects.

[17] see, International Committee of the Red Cross (2021) "Avoiding civilian harm from military cyber operations during armed conflicts," *International Committee of the Red Cross*, 26 May. Available at: https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations.

BIBLIOGRAPHY

1. *Twenty years on International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts* (2021). Available at: https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913.

2. International Committee of the Red Cross (2010) "Cyber warfare," *International Committee of the Red Cross*, 29 October. Available at: https://www.icrc.org/en/document/cyber-warfare.

3. International Committee of the Red Cross (2019) "International humanitarian law and cyber operations during armed conflicts," *International Committee of the Red Cross*, 28 November. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

4. Helen Durham, "Cyber Operations during Armed Conflict: 7 Essential Law and Policy Questions", Humanitarian Law and Policy Blog, 26 March 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions.

5. *Fundamental principles of IHL | How does law protect in war? - Online casebook* (no date). Available at: https://casebook.icrc.org/a_to_z/glossary/fundamental-principles-ihl.

6. Ayalew, Y. E. (2015). Cyber Warfare: A New Hullaballoo under International Humanitarian Law. Beijing Law Review, 6, 209-223. Available at: http://dx.doi.org/10.4236/blr.2015.64021

7. Secretary-General, Un. (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :: note /: by the Secretary-General*. Available

at: https://digitallibrary.un.org/record/799853?ln=en.

8. Pål Wrange, 'Intervention in national and private cyberspace and international law', Published in Jonas Ebbesson, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds), International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi, (Leiden: Brill/Nijhoff, 2014) 307-326. Available at: https://www.diva-portal.org/smash/get/diva2:778433/FULLTEXT01.pdf