Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
website: https: //rivierapublishing.id/JII/ index.php / jii /index

Cyber War and Civil Protection in the Perspective of International Humanitarian Law: Legal Challenges and Innovations in the Digital Age

Taufik Nur Cahyanto[1*], Adietya Yuni Nurtono[2], Tarsisius Susilo[3], Budiman Marpaung[4], Budi Saroso[5]
Sekolah Staff dan Komando TNI, Indonesia
toepexs@gmail.com

Keywords
Cyber War, International Humanitarian Law, Civil Protection, Tallinn Manual, Legal Innovation, Dual Infrastructure, Attribution

Abstract
The unregulated nature of cyber warfare under current international law is a widely recognized concern among experts calling for legal restrictions. A significant challenge lies in applying International Humanitarian Law (IHL) to protect civilians in this novel form of conflict. As digital infrastructure becomes an essential part of civilian life and military operations, the basic principles of HHI such as distinctiveness, proportionality, and prudence face significant obstacles in cyberspace. This article analyzes a variety of emerging legal ambiguities, including attribution issues, dual-use infrastructure, and non-physical impacts on civilians. In addition, this article explores legal innovations such as the reinterpretation of existing principles, the role of the Tallinn Manual, as well as the possibility of developing new legal instruments that are more adaptive to digital reality. The study concludes with policy recommendations to strengthen civil protection and enrich the cyber law architecture through multilateral cooperation and the development of new legal norms.

INTRODUCTION

In an era where digital networks penetrate almost every aspect of civil and military life, cyber warfare has emerged as a form of modern conflict that redefines the nature of the battlefield. Cyber warfare is identified as actions taken by parties engaged in conflict using various technological tools supported by technically skilled personnel. Essentially, cyber warfare aims to gain advantage by destroying, damaging, disabling, or seizing enemy systems.

While international security experts considered cyber warfare's potential, both within conventional conflict and independently, in the mid-1990s, the 9/11 attacks shifted priorities. The concept resurfaced in 2007, spurred by a major cyberattack on NATO member Estonia. Unlike conventional warfare involving kinetic force, cyber operations can cause highly destructive impacts without the direct use of physical violence.

The lack of coverage in international law literature regarding cyber warfare is a deeply concerning issue. Given that recent cyberattack models increasingly demonstrate readiness to engage in armed conflict, this concern is amplified by the emergence of other cyber groups prepared to conduct dangerous cyber operations against parties involved in armed conflicts. Whether or not countries around the world are prepared for this, cyber weapons have inevitably become a fundamental aspect of modern warfare. Disruptions to power grids, hospitals, or

public communications demonstrate that the cyber domain has a direct impact on civilian safety.

Prior studies have explored the intersection of cyber warfare and International Humanitarian Law (IHL), particularly concerning civilian protection. Sheraz and Dayan (2018) examined the applicability of IHL principles in cyber warfare, emphasizing the need for legal frameworks to address civilian protection in cyberspace. Similarly, Ayalew (2015) discussed the challenges of applying existing IHL norms to cyber conflicts, highlighting gaps in legal protections for civilians. Building upon these studies, the current research focuses on the practical implications of cyber operations on civilian infrastructure, analyzing recent incidents to assess the effectiveness of IHL in safeguarding civilian interests in the digital age.

This study aims to evaluate the extent to which International Humanitarian Law provides adequate protection for civilians against cyber warfare. Through an examination of recent cyber incidents affecting civilian infrastructure, the research endeavors to identify deficiencies in existing legal provisions and recommend modifications to enhance the safeguarding of civilian interests. The findings are expected to inform policymakers, legal practitioners, and cybersecurity professionals, contributing to the development of more robust legal protections and strategies to mitigate the impact of cyber warfare on civilian populations.

METHOD

This research is normative in nature, meaning that it does not collect data through interviews or surveys, but rather traces and analyzes the law as a system of norms. The main objective is to find solutions to legal problems through in-depth understanding of legal texts, basic principles, and opinions of legal experts. In its implementation, the statutory approach is used to understand the applicable laws and regulations; the comparative approach is used to compare legal regulations or practices from other countries or different legal systems; while the conceptual approach helps describe abstract concepts related to the legal issues under study.

The data sources used come from three types of legal materials. Primary materials have the highest authority because they are sourced directly from law-making institutions. Secondary materials help provide perspective and interpretation of primary materials. Meanwhile, tertiary material is a tool to clarify legal terms or concepts. The entire analysis was carried out through the method of literature study and documentary study, namely by reading, reviewing, and interpreting various existing legal documents. This approach is commonly used in legal research that aims to provide logical and systematic legal solutions or arguments.

RESULTS AND DISCUSSION

International Humanitarian Law (IHL) and the Tallinn Manual

International Humanitarian Law (IHL), or the law of armed conflict, is a set of rules designed to limit the impact of armed violence, particularly on individuals not directly involved in combat such as civilians, medical personnel and humanitarian workers. The aim is to ensure that even in the midst of war, humanitarian principles are respected. IHL emphasizes the importance of distinguishing between warring parties and civilian populations, prohibits the use of excessive force that could cause disproportionate harm to civilians, and demands caution in any military operation to minimize unnecessary damage. These provisions are set out in the Geneva Conventions of 1949 and the Additional Protocols of 1977, which form the main basis for the legal protection of victims of armed conflict at the international level.

The applicability of humanitarian law extends to armed conflicts occurring in both conventional and digital domains. This signifies that the established provisions and principles of humanitarian law are equally binding within cyberspace. The Martens Clause in humanitarian law offers a crucial legal basis for governing cyber warfare, even though it's a

recent development. This, combined with customary international law and other humanitarian law principles, ensures its applicability. Rule 20 of the Tallinn Manual specifically reflects this by detailing how humanitarian law extends to cyber operations during armed conflicts (Schmitt, 2013).

When cyberattacks on national critical infrastructure or critical information infrastructure (CII) result in human casualties, the Tallinn Manual's approach emphasizes the need to properly define and categorize them. Crucial factors like their direct nature and long-term effects lead Marcel Lettre to propose that cyberattacks resulting in human loss, injury, critical infrastructure damage, or substantial economic impact should be recognized as "acts of war" (Aftergood, 2017).

To determine whether a cyber attack can be categorized as a use of military force or as an "armed attack", Michael Schmitt proposes a stage of analysis that emphasizes the impact or consequences of the attack. This approach is in line with the methods used in the Tallinn Manual on the International Law Applicable to Cyber Warfare, which is an important reference in explaining the application of international law to cyber conflict. The categorization includes (Pipyros et al., 2016, 2017):

a. The severity of a cyberattack is measured based on the extent of the scope of the attack, how long the attack lasts, and how much intensity or strength of the cyber operations carried out;
b. The urgency of a cyberattack is judged by the immediacy of its consequences or impact;
c. Directness refers to how clear and direct the cause-and-effect relationship is between the actions in a cyber operation and the impact it causes;
d. Invasion refers to the level of disruption caused by cyber operations to the targeted country or cyber system, especially if the disruption is malicious or destructive in nature.;
e. Impact measurability implies that the more clear and quantitative the consequences of a cyber operation, the greater the ease with which a state can determine whether the attack meets the criteria of "use of force";
f. The military character is seen from the direct link between cyber operations and military operations. This linkage determines whether the cyber attack can be categorized as "use of force";
g. State involvement indicates the level of connection between a state entity and a cyber operation. The more transparent and close the link, the higher the probability of the cyberattack qualifying as a "use of force";
h. Presumptive legality refers to the adage that under international law, an action is essentially permissible unless explicitly prohibited. In the absence of a treaty provision or norm of customary international law specifically prohibiting an action, the action is generally presumed to have legal legitimacy.

This staging implies that not all cyberattacks are considered significant in terms of national defense. Therefore, not all cyber-attacks can be considered a form of "use of force." Just as the Tadić Case established the definition of "armed conflict" by referring to two main factors, namely the degree of violence and the extent to which the parties involved are organized, the assessment of cyberattacks also needs to be done using similar criteria (Prosecutor vs. Duško Tadić, 1997) cyberattacks are also assessed based on the conflict's intensity and the organization level of the actor involved.

It is important to remember that humanitarian law only applies in situations where there is armed conflict. Therefore, the applicability of this law is highly dependent on whether or not the conditions of armed conflict meet certain criteria, such as the intensity of violence and the organization of the conflicting parties. If cyberattacks do not reach a level sufficient to be considered part of an armed conflict, then humanitarian law cannot be applied in assessing or regulating such acts. However, this does not mean that there is no rule of law governing such

situations. Other positive laws, including international human rights law, remain relevant and applicable to protect the rights and obligations of parties in situations of non-armed conflict, including when facing cyberattacks.

In armed conflicts involving cyberattacks, not all civilians are automatically considered parties to the hostilities. The International Committee of the Red Cross developed the concept of "direct participation in hostilities" to provide a clear demarcation of when a civilian can be considered an active participant in the conflict. This concept is important because civilians who are not directly participating should be protected from attack, while those who are directly participating may lose special protection for as long as they are involved. The ICRC proposes three main elements that must be present for a person to be judged to be directly participating: first, there is a real threshold of harm resulting from his or her actions; second, his or her actions are the direct cause of the adverse effects on the opposing party; and third, his or her actions have a close connection to ongoing war or hostilities activities (Melzer, 2009). Although originally formulated for conventional warfare, the DPH concept remains relevant in cyber warfare (Rule 25 of the Tallinn Manual), where there is controversy regarding the "revolving door" phenomenon related to the preparation phase of individuals deemed to be directly participating in hostilities (Delerue, 2014).

Challenges of IHL in Facing Cyber Warfare

The challenges of International Humanitarian Law (IHL) in dealing with cyber warfare lie in adapting to rapidly evolving technology and the ambiguity in applying IHL principles to cyber operations. Cyber operations that can cause damage and suffering, even without the use of physical weapons, must still be governed by IHL. Another problem arises from the lack of an explicit and uniform definition of "attack." This ambiguity complicates the implementation of essential principles of international humanitarian law designed to manage armed conflict, including the principles of distinction, proportionality and the mitigation of unnecessary suffering. As cyberspace becomes increasingly integrated into modern military operations, various legal challenges arise, testing the limits of applicability and effectiveness of IHL. The unique characteristics of cyber warfare create complexity in assigning responsibility, ensuring civilian protection, and determining the scope and intensity of conflict.

National Regulations on Cyber Defense

In the face of increasingly complex security challenges in the digital era, especially cyber threats that can undermine the stability and sovereignty of a country, the government is taking strategic steps by making special regulations related to cyber defense. This regulation serves as an official guideline to regulate how the country should prepare and protect itself from cyber attacks that have the potential to disrupt the vital functions of national defense. The goal is to confront and ward off cyber attacks that can disrupt the implementation of national defense, so as to create a strong and effective cyber defense system.

Cyber-attacks are seen as criminal acts that fall within the realm of national security, making them the duty of law enforcement agencies such as the police. In general, there are various national laws and regulations that govern online activities. One of the challenges is that the Criminal Code, as the basic rule of criminal law in Indonesia, has not explicitly regulated cybercrime. However, with a broad interpretation approach, existing articles can be used to accommodate crimes involving intangible assets in the digital world. For example, in Article 362 of the Criminal Code, the term "property" can be interpreted not only as physical goods but also digital goods or data that have economic value. This approach allows the legal system to remain relevant and able to deal with cybercrime despite the lack of a separate regulation.

Furthermore, Law Number 11/2008 on Electronic Information and Transactions (UU ITE) fundamentally regulates internet-based activities. ITE Law was created to answer the need for more specific regulations related to the rapidly growing digital world and electronic transactions. This law regulates various activities that have the potential to cause cybercrime and provides a legal framework for law enforcement in the digital realm. In addition to regulating technical aspects such as illegal access and data interception, the Act also covers copyright protection as well as regulations in electronic commerce and consumer protection. With this broad scope, ITE Law is the main legal basis used to take action against cybercriminals, including various forms of attacks and manipulation of electronic data that can harm individuals, companies, and the state (Setiawan et al., 2018).

Then, Law Number 5 Year 2025 emphasizes the important role of the Indonesian National Army (TNI) in maintaining national defense, not only in war situations but also in the context of non-war threats, including cyber threats. Through Article 7, the TNI is given a special mandate in Military Operations Other Than War (OMSP) to actively participate in cyber defense efforts. This means that the TNI is not only tasked with conventional military operations, but also has a strategic responsibility in protecting the country's digital systems and infrastructure from cyber attacks that can endanger national security.

Ministry of Defense Regulation No. 82 of 2014 contains a more detailed definition of cyberattacks, namely:

> *"Any act, statement, or thought, whether intentional or unintentional, by any party, with any motive or purpose, carried out in any location, targeting electronic systems or their content (information), or equipment that relies heavily on technology and networks at any scale, against both vital and non-vital objects in military and non-military domains, that threatens national sovereignty, territorial integrity, and the safety of the nation."*

Cyber attacks may occur when the intensity and scale of cyber threats increase, changing from potential threats to actual threats. These are generally actions intended to access, control, modify, steal, damage, destroy, or disable systems or information assets. Such actions may take the form of cyber warfare, conducted deliberately and in a coordinated manner to disrupt national sovereignty, or cyber violence, which is unintentional, passive, and of a smaller scale.

Based on Appendix 2.2.a in the regulation, it provides a comprehensive overview of the various sources of cyber threats that can jeopardize state sovereignty. These threats come not only from abroad, but also from within the country, including actors such as extremist groups or organized criminal organizations, as well as hacktivist groups that use cyberattacks as a form of protest or activism. In addition, political conditions and conflicts can also trigger cyberattacks as part of competition or hostility. Furthermore, these threats can take the form of physical tampering with hardware through the installation of destructive tools, as well as more subtle activities such as infiltration and intervention in computer networks that can weaken or disrupt a country's digital defense system. In addition, cyber threats also come from malicious software (malware) that is generally spread via email with the aim of stealing data, damaging systems, manipulating information, or performing other harmful actions. Another threat is to the integrity of data or information, where the dissemination of specific information is done for specific purposes, such as in information warfare involving propaganda.

Based on the content of the regulation, it appears that there are no clear criteria to classify cyber attacks, including cyber terrorism, as acts of war or armed attacks. This is considered essential to be formulated, as such a classification could provide a legal basis for political leaders to authorize appropriate responses by military commanders or wartime leaders to existing cyber attacks (Cole et al., 2009; Haas & Fischer, 2020).

In addition to the aforementioned regulations, the Decree of the Minister of Defense No. KEP/1008/M/V/2017 is a strategic foundation in strengthening national defense to face challenges in the digital era, especially cyber threats. This policy does not only focus on military aspects, but also recognizes that cyber threats can be non-military and involve various sectors. Therefore, a comprehensive and integrated defense approach is needed, including the development of a strong national infrastructure and a universal defense system involving various elements of the nation. The integration of defense information systems enables effective coordination in the face of cyberattacks. In addition, this policy underlines the importance of improving technological capabilities in relevant ministries and institutions, developing human resources who are experts in the field of cyber defense, and building reliable information and communication technology infrastructure as a foundation for maintaining state security and sovereignty in the digital realm.

Based on the above regulations, it is evident that the current rules are still general in nature and need to incorporate a humanitarian law perspective—such as regulating what actions should be taken and how the state should respond in the event of cyber warfare. These considerations may include how to measure whether a cyber attack qualifies as an "armed attack" or can be categorized as a "use of force"; whether individuals engaging in online activities can be classified as combatants if their actions constitute direct participation in hostilities; and what specific policies the government will enact if a "use of force" occurs through cyberspace by a third party.

How Does International Humanitarian Law Respond?

When discussing when a cyberattack can be considered part of an armed conflict, it is important to incorporate International Humanitarian Law (IHL) into this study. IHL is crucial because it provides boundaries and rules on how states should act when facing conflict, including conflict in the cyber domain. By understanding and applying IHL, states can determine appropriate and internationally lawful responses to cyberattacks they experience. IHL itself is a part of public international law that focuses on controlling actions during war, with the primary goal of protecting victims and limiting excessive force. Within IHL, there are two important aspects: jus in bello, which governs behavior during war, and jus ad bellum, which addresses the legality of the use of military force.

Jus in bello is an important part of the law of war that regulates how warfare should be conducted and how war victims should be treated. It is traditionally regulated through two main groups of international treaties, namely the Geneva Conventions and the Hague Convention. The Geneva Conventions, which consist of four core treaties and two additional protocols, provide special protection to those directly affected in armed conflicts, such as wounded soldiers, prisoners of war, and civilians. Additional Protocol I emphasizes rules on the means and methods that can be used during warfare in order to minimize suffering. Meanwhile, the Hague Convention focuses on the technical and tactical aspects of warfare, such as the permissible use of weapons and tactics. It is important to note that these treaties must be interpreted broadly so that the scope of "armed conflict" is not limited to conventional forms. With this principle, humanitarian law emphasizes that anyone who is victimized in a conflict is entitled to legal protection in order to reduce the negative human impact of war.

Determining the definition of cyber weapons is an important step in regulating the laws and rules that apply to the use of cyber technology in conflict. Within the framework of International Humanitarian Law, if a cyber capability or tool is considered a weapon or method of warfare, it must be examined and regulated to conform to laws prohibiting the use of certain harmful or inhumane weapons. However, until now the international community has not reached a standardized agreement on what exactly constitutes a cyber weapon.

The few definitions that have been proposed reflect different perspectives on the nature and function of cyber weapons. One definition considers cyber weapons as tools that can cause physical harm to people or objects, including hardware and software used to carry out attacks.

Another definition highlights computer code designed to damage systems or living beings, either physically or mentally. Meanwhile, the view from the US Air Force emphasizes the function of such tools in injuring or incapacitating people and destroying property, even if the impact is temporary. A proper understanding of these definitions is essential for the rule of law to be properly and consistently applied to cyberattacks in the context of armed conflict.

It is important to understand that cyber capabilities used in conflict do not always take the form of hardware, but are often software or specific techniques that can cause serious damage or disruption. The US Air Force recognized this and provided a specific definition for cyber capabilities that includes any form of payload, whether hardware or software, designed to weaken or destroy an opponent's systems.

They also pioneered in regulating how these cyber capabilities must be legally vetted before use, ensuring compliance with international law. From the various definitions, there is agreement that cyber weapons are potentially dangerous and thus cyberattacks can be considered part of armed conflict, even if they are far removed from traditional methods of warfare. This demonstrates the challenge of international humanitarian law, which has yet to fully adapt to the rapid changes in digital technology. Therefore, the law needs to evolve in order to effectively regulate and protect humanity in the modern era influenced by cyber-attacks.

Additional Protocol I is an important part of international humanitarian law that governs international armed conflict. In the context of cyberattacks, this protocol is a reference that can be used to assess how the rules of IHL are applied. However, because some of its provisions are disputed and only bind states that agree to the treaty, the rules are not universally applicable to all states, posing challenges to the application of international law to cyberattacks at the global level.

Cyber weapons, like nuclear weapons, have unique characteristics that distinguish them from traditional weapons. As such, they require a rule of law tailored to their specific nature and effects. Although technically different, the effects caused by cyber weapons can be just as serious as physical weapons, so fundamental principles in IHL such as preventing excessive suffering and keeping attacks proportionate must still be upheld when dealing with cyber attacks. These principles ensure that even as technology changes, the humanitarian aspects of the laws of war remain protected.

The review of cyber weapons is difficult because states have full discretion to determine how and when they assess new weapons for compliance with the rules of international law, particularly IHL. Article 36 of the additional protocol to the Geneva Conventions stipulates the obligation of states to review new weapons so that they do not violate humanitarian law, but implementation is highly dependent on each state's interpretation and policy. Therefore, there is no international mechanism that strictly regulates when and how the review should take place, so flexibility and national policy are key. The ICRC emphasizes that these reviews should be carried out from the very beginning, from the research and development stage of the weapon, through to the procurement stage, to ensure there are no violations of the law from the start of development until the weapon is ready for use. This is important so that potential unlawful weapons can be stopped before they reach mass production or use.

As much of the development of cyber weapons is conducted in strict secrecy, the development process tends to be more dynamic and iterative compared to other conventional weapons. Cyber weapons are often designed for specialized purposes involving high technology and specific computer systems, so small changes to the code or mechanisms of such

weapons can produce different effects. For this reason, it is not enough for a legal review to be conducted only once when the weapon is first developed, but it must be updated every time there is a major change in the weapon's function or effect.

Legal counsel monitoring cyberweapons' compliance with the rule of law must be intimately familiar with these changes in order to provide appropriate guidance and prevent potential violations of the law. The role of legal advisors is crucial as they help ensure that the weapons developed remain compliant with the principles of international law governing armed conflict.

The review of cyber weapons in the context of International Humanitarian Law presents major challenges spanning legal, policy and practical implementation aspects. The existing discussion provides only a preliminary overview, signaling the need for more in-depth research and discussion in this area, given that there are still many uncertainties, including what the precise definition of "cyber weapons" should be. However, this does not mean that international humanitarian law cannot be used, rather it remains relevant and should be applied to new technologies such as cyber weapons. The Tallinn Manual is one important effort that has formulated legal guidance based on the current state of affairs, but there is still a need for states to adopt and develop these rules to become internationally recognized norms. Ultimately, the successful application of IHL to cyber weapons depends on the consensus and cooperation of the countries of the world.

While there is much conjecture as to how the content, interpretation and implementation of International Humanitarian Law (IHL) in relation to cyberweapons judicial review will evolve in the future, the author believes that this normative process will face major challenges. This is because cyber weapons exist in a very different environment from conventional weapons, with a high degree of secrecy and complexity. States often keep their cyberweapons activities secret, making it difficult for the international community to know exactly who is responsible for an attack or the use of such weapons. In addition, cyber technology allows perpetrators to conceal their identities in a variety of ways, making the process of tracking and proving very complicated. This makes establishing rules and implementing laws related to cyber weapons much more complex than traditional weapons.

In addition, some countries deliberately choose not to clarify the rule of law in cyberspace in order to be more flexible in carrying out their cyber operations and strategies. Since cyber weapons can be made with uncomplicated technology, this makes it easy for many countries to develop them without the need for large investments. As a result, it will be very difficult for the international community to agree on rules governing cyber weapons specifically. The international focus is more likely to be on establishing rules that protect critical infrastructure from cyberattacks, as this is a real threat that directly impacts national security. In addition, another challenge hindering the formulation of international rules is the absence of a clear and official definition of what a cyber weapon is, and also because the review of weapons is still the responsibility of individual countries, making it difficult to create binding global rules. All of these factors make regulating cyber weapons extremely complex and fraught with obstacles.

The essence of this statement is that although the technology and methods of warfare are constantly changing, including the advent of cyber warfare, the basic principles of International Humanitarian Law must still apply. "Armed conflict" is not just limited to the use of conventional weapons, but rather the impact and consequences of such actions, such as damage or loss of life. Therefore, to remain relevant, IHL needs to adapt to the development of new military technologies such as cyber weapons and ensure that the legal rules can still govern modern forms of conflict. The arms review process, which checks whether a weapon meets international legal standards, must be strengthened to ensure that IHL remains effective in

protecting humanity, while adapting to technological advances and changing global security conditions.

CONCLUSION

Cyber warfare presents a formidable challenge to the traditional scope of International Humanitarian Law (IHL), particularly concerning the protection of civilians. This study concludes that although the foundational principles of IHL—distinction, proportionality, and necessity—remain relevant, their application within the cyber domain demands urgent reinterpretation and legal adaptation. As cyber operations increasingly target critical civilian infrastructure, such as power grids and hospitals, the blurred lines between military and civilian targets expose non-combatants to disproportionate risks. The research affirms that while existing international legal frameworks offer a baseline for accountability, ambiguities in attribution, legal enforcement, and civilian safeguards persist. To ensure legal relevance and operational clarity, future research should explore the development of new IHL instruments tailored to cyber warfare. These should include cyber-specific protocols, mechanisms for international cooperation on attribution, and enhanced protection of civilian digital infrastructure. Strengthening legal literacy within national defense institutions and promoting regional cooperation, particularly in Southeast Asia, are also imperative. Overall, the legal community must pursue global consensus and legal innovation to uphold humanitarian values amid the complexities of digital conflict.

REFERENCES

Aftergood, S. (2017). What is an Act of War in Cyberspace? *Federation of American Scientists, Https://Fas. Org/Blogs/Secrecy/2017/10/War-Cyberspace*.

Buchan, R. (2016). Cyber warfare and the status of anonymous under international humanitarian law. Chinese Journal of International Law, 15(4), 741–772.

Cole, A., Drew, D. P., McLaughlin, R., & Mandsager, D. L. (2009). San Remo Handbook on Rules of Engagement. *San Remo Handbook on Rules of Engagement, Sanremo*.

Delerue, F. (2014). Civilian direct participation in cyber hostilities. *IDP: Revista de Internet, Derecho y Política= Revista d'Internet, Dret i Política*, *19*, 3–17.

Diantha, I. M. P. (2017). Metodologi penelitian hukum normatif dalam justifikasi teori hukum. Prenada Media Group.

Haas, M. C., & Fischer, S.-C. (2020). The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order. In *The transformation of targeted killing and international order* (pp. 107–132). Routledge.

Kelsey, J. T. G. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. Michigan Law Review, 1427–1451.

McCoubrey, H. (2019). International humanitarian law: Modern developments in the limitation of warfare. Routledge.

Melzer, N. (2009). *Interpretive Guidance on the Notion of Direct Participation in Hostilities under Internasional Humanitarian Law, Geneve: ICRC.*

Pipyros, K., Mitrou, L., & Gritzalis, D. (2017). Evaluating the effects of cyber-attacks on critical infrastructures in the context of Tallinn Manual. *Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory, Dept. of Informatics, Athens University of Economic and Business, Conference Paper*, *5*.

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law. *Information & Computer Security*, *24*(1), 38–52. https://doi.org/10.1108/ICS-12-2014-0081

Prosecutor v. Dusko Tadic, Case No. IT-94-1-T, Opinion and Judgment, 7 May 1997, paras. 561–562.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Setiawan, A., Wiwoho, J., & Rahayu, R. (2018). Strengtening Indonesia's Policy on National Cyber Security to deal with Cyber Warfare Threat. *South East Asia Journal of Contemporary Business, Economic and Law*, *15*(5).

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. Loyola of Los Angeles International and Comparative Law Review, 32, 303.