Veljković Sanela[*]
https://orcid.org/0009-0003-3650-290X

UDC: 341.33[355.4:004.738.5
Original scientific paper
DOI: 10.5937/ptp2403017V
Received on: February 12, 2024
Approved for publication on:
February 28, 2024
Pages: 17–28

POSSIBILITY OF APPLYING THE RULES OF INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE

ABSTRACT: Cyber warfare represents a new form of conflict in today's world. Unlike earlier traditional armed conflicts, cyber warfare is different in terms of means, methods, techniques, and actors. Cyber warfare takes place in virtual space through the use of information and communication technologies. The actors may be states, but also individuals who can inflict significant damage on their opponents. The consequences of cyber attacks may not be immediately apparent, but can manifest much later. Similarly, the outcome of a cyber attack can be material damage or the loss of human life. Since cyber operations can take place not only during conflicts but also in peacetime, the concept of cyber aggression is often present. States are aware of the new cyber threats and are developing their defensive and offensive capabilities, adopting strategies and doctrines addressing these issues. However, there is no international agreement that regulates the open issues related to cyber warfare, as there is no consensus among states on how to regulate it. There are attempts to apply the rules of international humanitarian law that govern armed conflicts to the realm of cyber warfare. Consensus within the international community has not been reached, leaving this area unregulated. The paper aims to examine the possibility of applying the rules of international humanitarian law, specifically the rules

[*]LLM, Junior Researcher, University of Belgrade, "Vinča" Institute of Nuclear Sciences, Belgrade, Serbia, e-mail: sanela.veljkovic@vin.bg.ac.rs.

governing the right to use force in international relations (jus ad bellum) and the rules governing the conduct of parties in conflict (jus in bello), to cyber warfare

***Keywords**: cyber warfare, cyberspace, jus ad bellum, jus in bello.*

1. Introduction

The 20th century is often marked as the century of armed conflicts. The First and Second World Wars resulted in a massive number of casualties, destruction, and the use of nuclear weapons. Concurrently, during the 20th century, there was a codification of rules limiting warfare actions. Over time, these rules have been developed and adapted to new humanitarian trends, and the commonly accepted term for this branch of law has become international humanitarian law of armed conflict (Petrović, 2010). Integral to this branch of international law is the right to the use of force (jus ad bellum) and the rules regulating the conduct of parties in conflict (jus in bello). The right to the use of force in international relations is restricted by Article 2(4) of the Charter of the United Nations. In situations where force is used, parties in conflict are obliged to respect the limitations imposed on them by the rules of international humanitarian law. The principles of distinction, proportionality, and military necessity represent the starting point for warfare actions. Given that the rules of international humanitarian law relate to armed conflicts, a particular challenge to these provisions is presented by cyber warfare as a new form of conflict. New threats to states emerge from cyberspace or the digital realm. The actors in cyber warfare are different from those in traditional armed conflicts. The means, methods, and weapons used in cyber warfare are not identical to those in previous conflicts. The goal of cyber warfare is not military superiority but rather information and the opponent's information and communication infrastructure. All of this can cause tremendous harm to the state that is the subject of the attack, so states today invest significantly in cyber security and develop their capacities. Although there are documents at the national level, it is not possible to achieve consensus on cyber warfare at the international level, so this issue remains unregulated. This paper examines the possibility of applying existing rules of international humanitarian law to cyber warfare. In addition to the introduction, the paper contains three more sections and a conclusion, along with a list of used literature and relevant documentation. The first part of the paper analyzes the concept of cyber warfare and its main characteristics. The second part discusses the rules of

international humanitarian law relating to the right to use force in international relations, as well as the possibility of their application to cyber warfare. The third part of the paper analyzes the principles of distinction, proportionality, and military necessity, as well as the possibility of their application to the field of cyber warfare.

2. Concept of Cyber Warfare and Its Main Characteristics

War is not foreign to human civilization. Its forms, methods, means, and techniques have changed throughout history. When talking about the existence of war or armed conflict, it implies the use of military capabilities of states in conflict. However, cyber warfare differs from traditional forms of armed conflict. Today, the existence of war does not necessarily require two armies to engage on the battlefield. Cyber warfare represents a "subset of information warfare, which does not require a traditional battlefield but attacks occur in cyberspace and are directed at enemy information and information and communication infrastructures" (Putnik, 2022, p. 69). Adkins (2001) defines cyber warfare as "the use of computer techniques of intrusion and other capabilities against the opponent's infrastructure based on information and communication technologies, with the intention of compromising national security or preparing for future operations against national security" (p. 13). There are numerous definitions of cyber warfare. According to one of them, cyber warfare represents "the use of state-sponsored weapons within the cyber domain to create problematic and destructive effects in the real world" (Raboin, 2011, p. 609). Cyber warfare is a conflict that takes place in cyberspace or the digital realm using information and communication technologies, aiming to affect the security of the attacked state and thus cause significant damage.

Cyber warfare, as a new form of conflict, does not have the same characteristics as traditional armed conflicts. "The most important characteristic of cyber warfare is that it takes place partially or entirely in cyberspace or through it (by acting from cyberspace on the physical world and vice versa)" (Mladenović, Jovanović & Drakulić, 2012, p. 91). Cyberspace is defined as "a human creation created by the application of information and communication technologies in the electromagnetic environment in which data are created, stored, sent, received, processed, and destroyed, whose elements are data, systems, processes, and people who are networked or can be networked" (Mladenović, 2016, p. 77). "Mastering information, establishing control over it, and the ability to create and present one's own perception of reality have promoted information as the primary object of cyber warfare, and cyber

warfare as the primary form of conflict" (Putnik, 2022, p. 90). On the other hand, information and communication infrastructures represent one of the primary objects of cyber warfare due to their connectivity with other critical infrastructures, which can cause enormous damage to the daily lives of the population of the attacked state (Vesić & Bjelajac, 2023, p. 85). What happens in cyberspace can "result in human casualties and material destruction in the physical world" (Putnik, Milošević & Bošković, 2017, p. 176).

Key differences between cyber warfare and traditional armed conflicts lie "in terms of the type of means, participants, and methods by which conflicts are waged" (Mladenović, 2016, p. 246). Based on the intentions or motives of cyber warfare subjects, as well as their threat-inducing techniques, the following classification of subjects has been made. Cyber warfare subjects include hackers, crackers, hacktivists, insiders, criminal groups, terrorists, corporations, national armies, and security services (Putnik, 2022, pp. 97-98). In traditional armed conflicts, subjects were embodied in states, while later conflicts were waged between states and certain armed groups on their territory. Today, cyber warfare subjects can be individuals and groups with the intention and desire to cause harm, as well as specific knowledge in cyberspace necessary for carrying out cyber attacks. For cyber warfare subjects, resources and geographic distance from the target of the attack do not pose difficulties for conducting cyber operations. Furthermore, practice has shown that it is very difficult to determine the identity of those behind cyber attacks, enabling subjects to evade responsibility for them. The use of cyber weapons will become increasingly common in the future compared to traditional kinetic weapons, considering the effects they have and their relatively low cost (Pool, 2013).

Regarding the methods and means of cyber warfare, they are not the same as the means and methods of traditional armed conflicts because cyber warfare is not waged on the battlefield but in cyberspace. There are several classifications of means and methods of cyber warfare in academic literature. Some authors classify cyber weapons as denial of service, malicious programs, logic bombs, IP address spoofing, and Trojan horses (Raboin, 2011). On the other hand, Professor Putnik (2022) divides the means and techniques of cyber warfare into those that are part of cyber attacks and propaganda operations. The means and techniques of cyber attacks include means for automated information gathering and conducting attacks (malicious code and service obstruction) and special techniques of individual deception (social engineering and phishing) (p. 82). These characteristics of cyber warfare, based on which this type of conflict differs from traditional armed conflicts,

pose major obstacles when attempting to apply the rules of international humanitarian law to cyber warfare. In the next part of the paper, the rules of international law relating to the right to use force in international relations (jus ad bellum) are presented, as well as the possibility of their application to cyber warfare.

3. Rules of International Law Jus Ad Bellum

Integral to the theory of just war are the rules regarding the right to use force in international relations (jus ad bellum). The right to use force is limited by the establishment of the United Nations. The Charter in Article 2(4) states that states "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations" (Charter of The United Nations, 1945). There are only two exceptions to this rule: the use of force in the case of self-defence under Article 51 and in situations where the Security Council considers there to be a threat to peace, a breach of peace, or an act of aggression under Chapter VII of the Charter. Since the United Nations Charter was adopted in 1945, its creators did not envision the possibility of using information and communication technologies and the internet for warfare purposes. When considering the right to use force in international relations, it is necessary to also consider the concept of aggression. Resolution 3314, adopted by the United Nations General Assembly in 1974, defines aggression as "the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state, or in any other manner inconsistent with the purposes of the United Nations Charter" (Definition of Aggression, 1974). Although specific acts of aggression are defined by the text of the Resolution, all of them are linked to the use of armed force. On the other hand, cyber warfare does not necessarily entail the use of armed force, nor does the subject necessarily have to be a state.

When interpreting the provisions of the Charter in the context of cyber warfare, a problem arises regarding whether a cyber attack can be classified as the use of force. Analyzing the compatibility of cyber attacks with the United Nations Charter, Schmitt (1999) concludes that existing rules of international law on the use of force (jus ad bellum) can be applied to cyber warfare. Cyber warfare has become a subject of interest not only for the academic community but also for states and certain organizations. States have recognized the potential for cyber warfare in the future and have begun to invest significant resources and efforts in this area, as well as to develop their own defensive and

offensive capabilities. Many regional organizations are interested in the field of cyber security and cyber warfare and actively work on cyber defence. The cyber attacks on Estonia in 2007 were particularly significant for NATO. These attacks represented a "kind of 'alarm' for NATO, as they demonstrated that entire states could be disabled and their sovereignty endangered by actions in cyberspace" (Putnik, 2022, p. 110). Within NATO, the Tallinn Manual on the International Law Applicable to Cyber Warfare (2017) was developed. The Tallinn Manual provides that "a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations, is unlawful" (pp. 42-43). Article 11 defines the use of force as follows: "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (p. 45). The level of the use of force is determined by the criteria of "scale and effects," referring to the Nicaragua v. United States case. Besides its immense value in terms of the potential application of the rules of international humanitarian law to cyber warfare, the manual does not represent a binding document that obliges states to act in a certain way in their mutual relations.

On the other hand, some authors believe that existing rules of international law on the use of force cannot be applied to the realm of cyber warfare and that it is necessary to establish a new set of legal rules to regulate this area.[1] Considering the possibilities of applying jus ad bellum rules to cyber warfare, some authors like Silver (2002) suggest that "efforts should be made towards adopting an international convention that would compel parties not to use attacks on computer networks for military or hostile purposes" (p. 94). However, it should be noted that whether the rules of jus ad bellum can or cannot be applied to the realm of cyber warfare, states in international relations should not act solely at their own discretion. This is supported by the advisory opinion of the International Court of Justice in the case of the Threat and Use of Nuclear Weapons, which states that "it cannot be concluded that existing principles and rules of humanitarian law do not apply to nuclear weapons. Such a conclusion would be inconsistent with the inherent humanitarian character of legal principles that permeate the entire law of armed conflict and apply to all types of wars and all types of weapons, those from the past, those from the present, and those from the future" (Legality of the Threat or Use of Nuclear

[1] For more see: Kilovaty, I. (2015). Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter. *Journal of Law and Cyber Warfare*, 4, 210-244.

Weapons: Advisory Opinion, 1996, par. 87). Although the consequences of cyber warfare and nuclear warfare are not comparable in scale, this advisory opinion can also be interpreted in the context of cyber warfare given that it is not regulated by new international instruments. However, the adoption and implementation of international treaties regulating a particular area depend on the will of states and their willingness to comply with the adopted provisions. Considering the historical inability to reach a consensus at the international level regarding cyber warfare, it seems that even in the event of adopting a potential cyber warfare treaty, it would face a fate similar to the Treaty on the Prohibition of Nuclear Weapons.

4. Rules of International Law Jus in Bello

International humanitarian law aims to regulate the conduct of parties during armed conflict, as well as the means and methods they have at their disposal. An integral and essential part of international humanitarian law consists of certain principles that parties to the conflict are obliged to respect. In this regard, this part of the work is dedicated to the principles of distinction, proportionality, and military necessity, as well as the possibility of their application to the realm of cyber warfare. The principle of distinction serves to protect civilians and civilian objects from attack. Parties to the conflict are obligated to carry out attacks only on military personnel and military objects. By the First Additional Protocol, military objectives are defined as objects: "which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" (Knežević-Predić, Avram & Ležaja, 2007, p. 210). The principle of proportionality is closely related to the principle of distinction and also serves to protect civilians and civilian objects. This principle stipulates that parties to the conflict "shall refrain from deciding to launch any attack which may be 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" (Knežević-Predić et al., 2007, p. 209). The principle of military necessity "permits measures that are actually necessary to achieve a legitimate military purpose and that are not otherwise prohibited by international humanitarian law" (International Committee of the Red Cross [ICRC], 2023). These principles are an integral part of the rules of international law (jus in bello) that regulate the conduct of parties in traditional armed conflicts.

However, when it comes to cyber warfare, it is questionable to what extent the aforementioned principles can be applied. Due to numerous differences compared to traditional armed conflicts, cyber warfare poses a serious challenge not only to the rules of international law jus ad bellum but also to the rules of international law jus in bello. As already mentioned, the objects of cyber warfare are information and information-communication infrastructure. During a cyber attack on the information communication infrastructure of a particular state, enormous damage can occur to its civilian population. Primarily because information-communication infrastructure is interconnected with other critical infrastructures in the state, an attack on it affects all others as well. Previous cyber attacks have shown the harmful consequences civilians can be exposed to. The outcome of cyber warfare is not only material damage but can also result in the loss of human lives. The question arises of how to differentiate between civilian and military in a situation of cyber warfare. Such a setup shows that cyber warfare is not only contrary to the principle of distinction but also to the principle of proportionality. When considering the principle of military necessity, it is unclear what measures are actually necessary to achieve a military purpose, as well as what happens if the purpose of a cyber attack is not purely military in nature.

In the Tallinn Manual on International Law (2017), which applies to cyber warfare, the principles of international humanitarian law are confirmed. According to Rule 31, "the principle of distinction applies to cyber operations" (p. 110). Rule 32 specifies that "the civilian population as such, as well as individual civilians, may not be the object of cyber attacks" (p. 113). The prohibition of attacks on civilian objects is governed by Rule 37, stating that "civilian objects may not be the object of cyber attacks. Computers, computer networks, and cyberinfrastructure may be the object of attack if they are military objectives" (p. 124). The principle of proportionality is defined by Rule 51: "Cyber-attacks which may result in 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, are prohibited" (p. 159). Since the manual is a product of the International Group of Experts, it does not compel states to adhere to these rules in the event of cyber warfare. Disagreements exist in both the international and academic communities regarding the application of international law rules to cyber warfare. Some authors argue that the principles of proportionality and distinction cannot adequately protect civilians and civilian populations in the context of cyber warfare and propose a solution in the form of adopting

Additional Protocol IV to the Geneva Conventions to regulate the field of cyber warfare (Pascucci, 2017, p. 460).

5. Conclusion

Cyber warfare as a new form of conflict today requires achieving consensus on an international level regarding its regulation. There are numerous differences compared to traditional armed conflicts, which are governed by the rules of international humanitarian law. The actors in cyber warfare are not only states or armed groups in a specific territory but can also be individuals. The targets and objectives of cyber warfare differ from those of traditional armed conflicts. Military superiority loses its significance and does not hold the same value in cyber warfare. Information and communication infrastructures in the twenty-first century gain significance that they did not previously have. Conflict has shifted from the battlefield to the digital or cyberspace, which is accessible to everyone. Remaining anonymous on this "new" battlefield creates difficulties in determining the identity of the attacker and their responsibility. Geographical proximity loses its former importance for conducting cyber operations because attacks can come from any part of the world. The weapons used in cyber warfare are entirely different from those used in traditional armed conflicts. Their cost is much lower than that of traditional kinetic weapons, making them easily accessible to anyone. The only similarity between cyber warfare and traditional armed conflicts may be their outcome, namely loss of human lives and significant material damage. There is no consensus on an international level, although states are aware of new cyber threats and the importance of cyber security today. In this regard, states develop their defensive and offensive capacities, establish various bodies dealing with this area, and adopt numerous documents at both the national and regional levels. Regarding the possibility of applying the rules of international humanitarian law to cyber warfare, there is no consensus even within the academic community. Some authors advocate for the application of jus ad bellum and jus in bello rules to cyber warfare, while others advocate for the adoption of a completely new legal framework to regulate this area. The Tallinn Manual, initiated by NATO, is of great value in considering the aforementioned issue and can serve as a model for the development of a binding international instrument. When analyzing the possibility of applying the rules of international humanitarian law to cyber warfare, it is essential to consider the differences between cyber warfare and traditional armed conflicts. The application of the jus ad bellum rules indicates that in each individual situation,

the threshold of force used during a cyber attack should be considered, while the application of the jus in bello rules shows that it is challenging to adhere to traditional principles of distinction and proportionality when it comes to cyber warfare. The best solution would be the adoption of a completely new international document regulating the entire field of cyber warfare. However, given the previous stance of states, it is questionable whether such an international instrument would be adopted at all, and if adopted, whether it might suffer the fate of the Treaty on the Prohibition of Nuclear Weapons. Certainly, states cannot act as they wish, not even in the field of cyber warfare, which is still not regulated at the international level. This is supported by both paragraph 87 of the advisory opinion of the International Court of Justice in the Case Concerning the Threat or Use of Nuclear Weapons and the Martens Clause, which is of immense importance in situations of the absence of written law.

Acknowledgements: This work was conducted as part of the scientific research activities at the 'Vinča' Institute of Nuclear Sciences, an institution of national significance for the Republic of Serbia. It was funded by the Ministry of Science, Technology, and Innovation under grant number: 451-03-66/2024-03/ 200017.

Veljković Sanela
Univerzitet u Beogradu, Institut za nuklearne nauke „Vinča", Beograd, Srbija

MOGUĆNOST PRIMENE PRAVILA MEĐUNARODNOG HUMANITARNOG PRAVA NA SAJBER RAT

APSTRAKT: Sajber rat predstavlja novi vid sukoba današnjice. Naspram ranijih tradicionalnih oružanih sukoba, sajber rat je drugačiji po sredstvima, metodama, tehnikama i akterima. Sajber ratovanje se odigrava u virtuelnom prostoru upotrebom informaciono-komunikacionih tehnologija. Akteri mogu biti države, ali i pojedinci koji mogu da nanesu ogromnu štetu protivniku. Posledice sajber napada ne moraju da budu odmah očigledne, već se one mogu dosta kasnije ispoljiti. Isto tako, rezultat sajber napada

može biti šteta materijalne prirode ili gubitak ljudskih života. S obzirom da se sajber operacije ne moraju izvoditi samo tokom trajanja sukoba, već i u periodu mira, neretko je prisutan i pojam sajber agresije. Države su svesne novih sajber pretnji te razvijaju svoje defanzivne i ofanzivne kapacitete i usvajaju strategije i doktrine koje se bave ovim pitanjem. Međutim, na međunarodnom planu ne postoji dokument koji bi regulisao otvorena pitanja u vezi sa sajber ratom jer ne postoji saglasnost među državama povodom načina njegovog regulisanja. Postoje pokušaji da se pravila međunarodnog humanitarnog prava koja regulišu oružane sukobe primene na oblast sajber ratovanja. Konsenzus u međunarodnoj zajednici nije postignut, te ova oblast ostaje neregulisana. Rad teži da ispita mogućnost primene pravila međunarodnog humanitarnog prava, odnosno pravila koja regulišu pravo na upotrebu sile u međunarodnim odnosima (jus ad bellum) i pravila koja regulišu ponašanje strana u sukobu (jus in bello) na sajber rat.

***Ključne reči**: sajber ratovanje, sajber prostor, jus ad bellum, jus in bello.*

References

1. Adkins, N. B. (2001). *The Spectrum of Cyber Conflict From Hacking to Information Warfare: What is Law Enforcement's Role?* Alabama: Air Command and Staff College, Air University
2. Charter of The United Nations, UN, 1945. Downloaded 2024, January 15 from: https://treaties.un.org/doc/publication/ctc/uncharter.pdf
3. Definition of Agression, United Nations General Assembly Resolution 3314 (XXIX), 1974. Downloaded 2024, January 15 from: https://iilj.org/wp-content/uploads/2016/08/General-Assembly-Resolution-3314.pdf
4. Kilovaty, I. (2015). Rethinking the prohibition on the use of force in the light of economic cyber warfare: towards a broader scope of Article 2 (4) of the UN Charter. *Journal of Law and Cyber Warfare, 4*, pp. 210–244
5. Knežević-Predić, V., Avram, S., & Ležaja, Ž. (2007). *Izvori međunarodnog humanitarnog prava* [*Sources of international humanitarian law*]. Beograd: Publikum
6. Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion, International Court of Justice, 1996. Downloaded 2024, January 15 from: https://www.icj-cij.org/sites/default/files/case-related/95/7497.pdf
7. *Military necessity, How does law protect in war? – Online casebook*, ICRC. Downloaded 2024, January 15 from: https://casebook.icrc.org/a_to_z/glossary/military-necessity

8. Mladenović, D. D. (2016). *Multidisciplinarni aspekti sajber ratovanja – doktorska disertacija* [*Multidisciplinary aspects of cyber warfare – doctoral thesis*]. Beograd: Fakultet organizacionih nauka
9. Mladenović, D. D., Jovanović, M. D., & Drakulić, M. S. (2012). Definisanje sajber ratovanja [Defining of cyber warfare]. *Vojnotehnički glasnik, 60*(2), pp. 84–117. DOI: 10.2298/vojtehg1202084M
10. Pascucci, P. (2017). Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution. *Minnesota Journal of International Law, 26(*2), pp. 419–460
11. Petrović, M. (2010). Međunarodno ratno i/ili humanitarno pravo [International law of war or humanitarian law]. *Pravo–teorija i praksa, 7*(8), pp. 178–185
12. Pool, P. (2013). War of the cyber world: The law of cyber warfare. *The International Lawyer 47*(2), pp. 299–323
13. Putnik, N. (2022). *Sajber rat i sajber mir* [*Cyber warfare and cyber peace*]. Beograd: Univerzitet u Beogradu – Inovacioni centar Fakulteta bezbednosti i Akademska misao
14. Putnik, N., Milošević, M., & Bošković, M. (2017). Strateško planiranje sajber odbrane – ka adekvatnijem pravnom okviru i novoj koncepciji procene rizika, izazova i pretnji [Strategic planning of cyber defence – toward a more adequate legal framework and a new concept of risk assessment, challenges, and threats]. *Vojno delo, 69*(7), pp. 174–185. DOI: 10.5937/vojdelo1707174P
15. Raboin, B. (2011). Corresponding evolution: international law and the emergence of cyber warfare. *J. Nat'l Ass'n Admin. L. Judiciary, 31*(2), pp. 602–668
16. Schmitt, M. N. (1999) Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *The Columbia Journal of Transnational Law, 37*, pp. 885–937
17. Silver, D. B. (2002). Computer network attack as a use of force under Article 2 (4) of the United Nations Charter. *International Law Studies, 76*(1), pp. 73–97
18. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2017. Downloaded 2024, January 15 from: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf
19. Vesic, S., & Bjelajac, M. (2023). Cyber security of a critical infrastructure. *Pravo – teorija i praksa., 40*(77), pp. 77–88. DOI: 10.5937/ptp2302077V