Academician Miodrag N. SIMOVIĆ, PhD[*]
Constitutional Court of
Bosnia and Herzegovina, Judge
Faculty of Law, University of Banja Luka,
Full Professor
Academy of Sciences and Art of
Bosnia and Herzegovina, Active Member
European Academy of Sciences and Arts, Active Member
Russian Academy of Natural Science, Foreign Member

Original Scientific Article
Received:1 October 2020
Accepted: 2 November 2020
UDK: 341.48
343.43/.45:004.738.5
https://doi.org/10.47152/rkkp.58.3.2

Živorad RAŠEVIĆ, PhD
Assistant Professor, MA (King's College London), CMgr FCMI,
Lieutenant Colonel, Legal service, Bosnia and Herzegovina Armed Forces

Vladimir M. SIMOVIĆ, PhD
Prosecutor's Office of Bosnia and Herzegovina, Prosecutor
Faculty of Security and Protection,
Independent University in Banja Luka, Associate Professor
Faculty of Law, University „Vitez" in Vitez, Associate Professor

CYBER WARFARE AND INTERNATIONAL CYBER LAW: WHITHER?

This paper analyses historical, sociological and normative aspects of the cyber violence in international relations and international law, aiming to assess the adequacy of the extant international norms for its regulation. It results with the knowledge on the lack of international cooperation and a universal approach, the instrumentalisation of the internet as a means of warfare, lacunae in the relevant legal framework, and the peril of compromisation of the international law. Since the social

[*] e-mail: vlado_s@blic.net

jeopardy of activities in the cyberspace is hardly measurable and subjected to highly arbitrary interpretations, the problem of the uncertain peacetime or belligerent legal qualification of cyber activities is exposed. The other serios problem is a high risk from potentially disproportional responses of states to the cyber violence. Especially due to the lack of universal international institutions in the field of cyber, it must be concluded that the international lege lata applicable to the cyber violence is not adequate and sustainable. The progressive development of international cyber law is thus suggested, through the pacification of the internet and the international criminalisation of cyber violence.

Key words: Internet, Cyber warfare, Cyber law, Lawfare

1. Introduction

Accelerated technological development and the global spread of the Internet is certainly one of the greatest contemporary challenges international law is facing. New means and ways of communication are changing the nature of relations between people and states, and extensive legally-theoretical and scientific elaborations of these changes have resulted in knowledge of the accompanying global threats that deserve the attention and reaction of the entire international community.

However, these findings did not lead to the defining of a comprehensive positive legal framework and the systematization of legal discipline that would comprehensively regulate this emerging area of legal transactions, which is already commonly known as Cyber law. This incoherence and incompleteness is certainly the result of competition between states in the accumulation of benefits provided by a new area of communication, as much as the attitude of science that a new legal regime is not needed, i.e. that existing law can successfully regulate this area. The inadequacy of legal regulation is particularly problematic in international law of war. It points out that this is an area of conflict where there are no laws (Gervais, 2012: 579) and proposes the adoption of a convention on cyber weapons or at least a more general conventions on Internet security, in order to reduce the threats cyber attacks represent (Geers, 2010: 547-551).

Applying historical, sociological and dogmatic methods, this paper analyzes the dilemma between the need for a new legal framework and the retention of the existing one, by focusing on the legal regulation of the use of Internet-mediated violence in peace and war. In the first part, the basic concepts and tendencies related to cyber warfare in the practice and theory of international relations are presented. The second part presents and explains the international legal framework for the use of

force by using the Internet, including both groups of rules of war (*ad bellum* and *in bello*). The third part summarizes the social, normative and ethical aspects of the legal regulation of cyber warfare and proposes a solution to the dilemma.

2. Internet and interpretation of contemporary wars

To understand the status and function of international norms related to the area of violent use of the Internet in peace and war, it is necessary to shed light on the historical, doctrinal and social context of contemporary conflicts. About that below.

When we talk about the Internet, we should always keep in mind that this is a deeply militarized phenomenon. Namely, it is an incidental product of the development of science and technology of the Cold War, which arose as a result of the efforts of the American Government to ensure the sustainability of the communication system in the circumstances of a possible nuclear attack. In this context, the destructive potential of purpose-designed softwares for disabling opponents' computer networks was also noted (Gervais, 2012: 527-531).

Electronic spectrum control is considered as an important aspect of the internal sovereignty of states, in particular of the formed forces for electronic warfare that have been existing in all contemporary armed forces for several decades. Therefore, in military doctrines governing the rules of use of force around the world, the concept of Cyber warfare as an element of comprehensive war efforts has been developed, which means the use of military force by cyber means and methods. Cyber warfare is considered as an important aspect of Hybrid warfare. This concept encompasses the means, methods and goals of warfare that deviate from traditional settings insofar as they are conducted in a gray zone in which the already blurred line of demarcation between war and peace is lost. In short, hybrid warfare combines classic military warfare with diplomatic, economic, intelligence, and electronic means and methods – for political and economic pressure and to achieve desirable psychological effects. This modern way of warfare includes „conventional capacities, irregular tactics and formations, terrorist acts, including non-discriminatory violence and coercion, criminal disorder, perpetrated by the parties to the conflict and non-state actors." (Wither, 2020: 8).

As the question of the legality of cyber warfare remains unresolved (Gervais, 2012: 526) – which can certainly be concluded for other aspects of hybrid warfare – it is necessary to legally justify such problematic activities. To this end, a new aspect of hybrid warfare called Lawfare has been developed. This complex word – perhaps more appropriate to argue *contradictio in adjecto* or even oxymoron

– was coined in 1975 in the context of criticisms of excessive and inhumane application of adversarial judicial procedures.[1] This concept was introduced into the world of military doctrine by the American general and lawyer Charles Dunlap at the beginning of this century to mark the abuse of the right to achieve military goals and define it as a first-class factor of modern military interventions (Dunlap, 2002: 2-4). The mentioned method of warfare is used to label other as an enemy for making senseless the principles on which the law is based and to justify the consequent aggressive reaction against it, allegedly for the purpose of affirming the law. It is an increasingly widespread aspect of hybrid warfare that exerts an impact that is analogous to physical effects (Mosquera, 2016: 72-73).

The examples of cyber violence cited in the literature confirm the intertwining and conditionality of the presented concepts, subjective approach and crucial role of the war narrative in their interpretation. Thus, in 2007 in Estonia, after the riots caused by the Russian minority due to the demolition of monument to Soviet soldiers, the internet structure of the government and banks were attacked with malicious software. Sources of harmful activities were widespread, including the territory of Russia, and caused economic and social damage.

In 2008, the American-sponsored media Radio Free Europe was attacked in a similar manner in Belarus, and the domestic government was suspected of endangering the basic human right to freedom of expression by not fulfilling its duties. In the same year, after the adoption of the Law Banning the Display of Soviet Symbols, the government infrastructure in Lithuania was damaged, and a Russian nationalist hacker group was suspected. At the same time, during the armed conflict between Russia and Georgia, numerous harmful effects on the cyber structure of Georgian institutions were reported and possible causers from the territory of Russia (Tikk, Kaska, Vihul, 2010: 14-89). In 2010, a computer virus called Styxnet was discovered in an Iranian nuclear plant, and suspicions were directed at Israel and the United States (Roscini, 2014: 6-7). Recent examples include allegations that a virus of American origin was spotted in the software of the Russian power grid[2] and that China is hacking the governments of the countries of the Asia-Pacific region.[3]

---

1 „As inquisitorial or investigative technique is abandoned, only adversarial or prosecutorial procedures apply. The search for truth has been replaced by the classification of objects and the perfection of fight. In legal warfare (...) a duel is fought with words, not swords. Is that enough?" (Carlson, Yeomans, 1975: 5)

2 Sanger, D. E., Perlroth, N. (2019, June 15th) U.S. Escalates Online Attacks on Russia's Power Grid, The New York Times, available at: *https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html* accessed on 05.06.2020.

3 Kharpal, A. (2020, May 7th) New cybersecurity report says China-based group is hacking Asia-Pacific governments, CNBC, available at*:* *https://www.cnbc.com/2020/05/07/chinese-hacking-group-naikon-reportedly-spyingon-asia-governments.html* accessed on 05.06.2020.

On the day of writing this paper, according to the expertise of the business entity CheckPoint Software Technologies, which publishes data in real time, over 14 million cyber attacks were recorded.[4] It is pointed out that cyber attacks have great advantages over classical ones, because they are cheap, long-range, fast and powerful tactics of coercion or destruction, often without the possibility of prosecution (Gervais, 2012: 579). War rhetoric, concern about the enormous destructive potential of the Internet, and frequent new accusations against unidentified perpetrators and states, sketch a disturbing landscape of escalating confrontations that are dispersed in all spheres of public and private life.

When the concepts presented are analyzed in the light of traditional theories of international relations, the dilemma between the *status quo* and the need for the progressive development of this branch of law – seems more difficult, but still somewhat clearer. Any proponent of realism in international relations – especially those states seeking to maintain global leadership positions – would in principle consider that cyber warfare opens up new possibilities for strengthening of state power, while liberal internationalists would insist on legal regulation of international cooperation.

In short, cyber violence in contemporary international relations is as much more present as it is increasingly controversial. The dominant theoretical approach to this problem is colored more realistically than internationalistically liberal, as states prioritize the search for possibilities to use the Internet to strengthen their positions in the global competition for resources in a new area of communication. That is why the traditional notions of war, peace, military intervention and the function of law have changed beyond recognition. The question is whether this is a perversion that should not be accepted, or still be practical and seek benefits in the dominant interpretations of violent use of the Internet?

3. International regulation of cyber violence

After enlightening the status and development of cyber warfare in contemporary military doctrines and international relations, this part of the Paper analyzes the responses of international law and science to this phenomenon. We will first talk about the sources of international law related to cyber violence, and then about their place in the legal system.

The social danger of cyber violence is recognized and criminalized in the internal rights of many states. Moreover, the international character of computer

4 Live Cyber Threat Map, available at: *https://threatmap.checkpoint.com/* accessed on 04.06.2020.

crime has contributed to the globalization of law, as it has initiated the process of transposing legal solutions from international law into national legislation (Dabović, 2007: 52-53).

However, this process has left little trace in regulating relations between states. One universal and one regional treaty are cited as the only international sources in this regard. First, the UN Convention against Transnational Organized Crime (Palermo, 15.11.2000)[5] in Articles 14 and 29 obliges states to train law enforcement agencies and to cooperate with other states against transnational organized crime perpetrated by using computers.

The Council of Europe Convention on Cybercrime and the Additional Protocol on the Punishment of Racist and Xenophobic Acts through Computer Systems are in force in the European theatre (Budapest, 23 November 2001).[6] This exemplary regional instrument obliges signatory states to criminalize the illegal use of computer networks and electronic systems, and to cooperate in criminal prosecution. Therefore, the states are in charge of suppressing computer violence, and criminal law repression and international cooperation have been chosen as an adequate remedy.

For now, the only attempt to compile a comprehensive catalogue of applicable international rules that apply in both war and peacetime circumstances is the Handbook on International Law Applicable to Cyber Operations (hereinafter: the Tallinn Handbook), compiled by a group of eminent international law and technical experts, under the auspices of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn (Schmitt, 2017). This unofficial document, drafted under the auspices of a military-political regional organization, certainly does not belong to the formal sources of international law defined in Article 38 paragraph 1 of the Statute of the International Court of Justice, but has some international legal relevance due to the ambition of drafter to express relevant rules in the field of international public law by the authority of legal profession. In this sense, the claims that this is an interpretation of the *lex lata* by independent experts who have impartially expressed and harmonized their opinions on which customary and contractual law is applicable to the Internet can be taken seriously (Schmitt, 2017: 3-5). Therefore, this document can be used as a useful and reliable additional means of concretizing the principles of international law, filling legal gaps and interpreting applicable norms. At the same time, it should not be forgotten that it does not express the legal views and opinions of a large part of legal experts and subjects of international law.

5 Ratified in BiH („Official Gazette of BiH-International Treaties", Number 03/02).

6 Ratified in BiH („Official Gazette of BiH-International Treaties , Number 6/06).

So, at the moment, we can talk about international law applicable to the Internet or about emerging international cyber law, which for now contains rare and mostly regional contractual norms governing cyber violence. When this violence crosses the borders of peace, cyber warfare law should be classified under the umbrella term Operational Law. This legal discipline, which is almost unknown in our country, has been developed in the Western tradition of the rule of law, which has as its subject the legality of military command in decision-making and execution of military operations (Rašević, 2017: 25-26).

The application of the general rules of international law leaves a wide space for the creative application of law, but creates legal uncertainty due to the lack of knowledge about a new type of communication. The question is to what extent is this *status quo* appropriate when the cyber damage is so great that it undermines state sovereignty or has a detrimental effect on the political, economic and social life of both individual states and the international community?

4. Cyber violence in the grey zone of international law

Clear legal qualifications and reactions of subjects of international law are needed to solve the problem of spreading of cyber violence and its international legal consequences. In order to be legitimate, those reactions should be appropriate and proportionate to the degree of social danger. In the case of cyber violence, this challenge seems to be too difficult for current international law due to erasing of the boundaries between peace and war.

When violence undermines the foundations of the community, two sets of rules come into force, according to the division established by Grotius: the first determines when the state can resort to armed force (*ius ad bellum*) and the second one how to use that force (*ius in bello*). In short, the modern *ius ad bellum* is contained in Artice 2 paragraphs 4 and 51 and Chapter VII of the UN Charter (1945): the threat of force and its use in international relations are prohibited, with the exception of self-defense and an explicit order of the Security Council. Moreover, aggression is criminalized as a crime against peace by the Amendment to the Rome Statute of the International Criminal Tribunal, Kampala 2011 (Rašević, Vlajnić, 2020: 661-681).

On the other hand, *ius in bello* is contained in international humanitarian law, which limits the use of armed violence in accordance with the principles of humanity, distinction between combatants and civilians, proportionality between violence and expected military advantages (Henckaerts, Doswald-Beck, 2005: 3-80). The norms of international humanitarian law give closer indications of the

problematic line of demarcation between peacetime circumstances, non-international and international armed conflict (Edlinger, 2016: 39-45). Below, on the applicability of these norms to the field of the Internet.

4.1. Between war and peace

The transition of violence to the sphere of war, from which the modern *ius ad bellum* in principle distracts by the prohibition of aggression, is defined by the provisions of joint Article 3 of the Geneva Conventions (1949) and Article 1 of Protocol No. II on Protection of Victims of Non-International Armed Conflicts (1977).[7] In short, the threshold of war is crossed if an armed conflict is fought in the „territory of the High Contracting Party between its armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory that allows them to conduct continuous and directed military operations..." On the other hand, there can be no talk of armed conflict if the violence is limited to „situations of internal riots and tensions, such as rebellion, isolated and sporadic acts of violence and other acts of a similar nature..."

This distinction is particularly important for the purposes of this analysis, as the possibility has been accepted in the literature that cyber violence may meet these criteria (Sanders, 2018: 521). The Tallinn Book proposes the threshold for transition from peace and war as follows: "... when there is prolonged armed violence, which may include or be limited to cyber operations, between government armed forces and organized groups, or between such groups. Confrontation must reach a minimum level of intensity and the parties involved in the conflict must have a minimum level of organization." The criterion defined in this way is not very helpful due to the use of broad and vague terms, and the expert group that formulated this rule could not agree whether threshold is crossed when non-destructive activity on the Internet is carried out in circumstances of civil riots. There was also no consensus when discussing whether the criterion of a minimum level of organization was met when cyber operations are conducted by virtual groups and mutually uncoordinated individuals (Schmitt, 2017: 385-391).

The consequences of crossing this threshold are really severe, because the act of internet-mediated violence can be qualified as an armed attack[8] that authorizes

7 "Official Gazette of FNRY" Number 24/50 and „Official Gazette of SFRY-International Treaties" Number 16/78.

8 "The term 'attacks' means acts of violence against opponents, whether offensive or defensive. "Article 49 of Additional Protocol 1 to the Geneva Conventions for the Protection of Victims of International Armed Conflicts.". (See also Schmitt, Garraway, Dinstein, 2006: 7).

the state to resort to cyber and even physical force by invoking self-defense from Article 51 of the UN Charter.[9] In other words, violence caused by the use of the Internet ceases to be subject to a peacetime set of rules that treats it as a crime and moves into the domain of regulation by international humanitarian law. Then, a peacetime criminal becomes a fighter, because such acts lose the character of illegality if they are characterized as a means or method of warfare that are not explicitly prohibited by the norms of humanitarian law. As suggested in the Tallinn Book, such qualified internet fighter can also become a war criminal.[10] This is quite understandable, because the provisions of international and domestic criminal law are set wide enough to cover both these means and methods of warfare.

Legal uncertainty regarding the choice to apply the norms of peacetime or war law is a logical consequence of contradictions and unsystematization of international law, which on the one hand prohibits war, and on the other regulates its outbreak and conduct by widely set institutes of humanitarian law. This uncertainty is further deepened in the case of Internet-mediated violence, because there is no universally competent international institution with necessary technical knowledge to set global standards, and in specific cases to impartially determine the causality and responsible perpetrator. In the absence of such an institution, biased expertise and arbitrary accusations dominate the public discourse. This raises a justified fear that any violent activity via Internet may be qualified as war operation, aggression or war crime. Moreover, such a qualification may provoke a reaction by armed force against individuals, groups, or state that are labelled as enemies for their alleged responsibility for Internet-mediated activity.

The danger of cyber violence is that it can be easily misused as a motive and means of conducting hybrid and legal war. Unlike universally established institutions and mechanisms for monitoring and controlling conventional, nuclear, chemical and other weapons, the Internet as a weapon continues to exist in an international legal vacuum. There are no clear criteria for assessing whether a certain internet-mediated action is a peacetime crime or a way of warfare, nor whether the state should react according to peacetime or war rules. A wide space is open for arbitrary and subjective interpretations to the extent that everything comes down to the question: „is it in your interest to declare that this is an act of war?" (Libicki, 2009: 182).

9 "A state that is the target of a cyber operation that reaches the level of an armed attack can use its inherent right to self-defense. Whether a cyber operation is an armed attack depends on its severity and effect." (Schmitt, 2017: 339).

10 "Cyber operations may be various war crimes under individual criminal responsibility according to international law." (Schmitt, 2017: 391-396).

4.2. Between international and internal armed conflict

The cited norms of humanitarian law also outline the lines of demarcation between international and non-international armed conflict. This is also important in this context, because "conflict classification determines specific sets of rules that apply to the conduct of military operations" (ICRC, 2013: 55). The dilemmas that arise by the use of cyber violence in undoubtedly confirmed war circumstances are no easier. Namely, military cyber or physical reaction to Internet-mediated violence can escalate into an international armed conflict only if the enemy state is clearly identified, i.e. a certain act of cyber violence is attributed to a certain state.[11]

The trouble is that there are no universally accepted and binding international norms regarding the responsibility of the state for illegal actions. It remains to refer to the provisions of the Rules of State Responsibility formulated by the International Legal Commission and recommended by the UN General Assembly.[12] This is done by the Tallinn Book, faithfully transposing the provisions of this document into Rules 14-19 regulating the responsibility of states for cyber violence committed by state bodies and non-state actors and exceptions in the form of consent of the attacked state, self-defense, countermeasures, necessity, *force majeure* and trouble (Schmitt, 2017: 79-111).

In addition to the difficulties in proving the causality between the action of a state body and the damage caused by use of Internet, it is especially problematic to attribute responsibility to the state for cyber operations of non-state actors in Rule 17. According to this rule, a certain state becomes an enemy of war if the perpetrators have operated according to instructions, guidelines or under the control of the state, and the state recognizes and accepts that operation as its own. The mentioned provision opens space for contradictory interpretations, such as those related to the responsibility of the Kingdom of Serbia for the murder of the Archduke in 1914 in Sarajevo. Without arguing that such an imprecise rule is better than none, the question arises as to how to prove doubts about a state's connection to hacker groups when an independent and impartial investigation can hardly be conducted in circumstances of growing tensions with a state labelled in advance as hostile.

---

11 It is proposed to characterize an international conflict as follows: "... when there are hostilities involving or limited to cyber operations between two or more states." (Schmitt, 2017: 379)

12 The Articles on State Responsibility. UN General Assembly, GA Res. 56/83, UN Doc. A/ RES/ 56/83 (12 December 2001)

4.3. Status quo or progressive development of international cyber law?

There is no resolute answer to the question in the title, given that convincing but contradictory arguments are presented here. They have been re-evaluated here to suggest an answer based on the need to affirm the fundamental values of international law.

The disturbing landscape of global cyber confrontations is further complicated by legal uncertainty both in terms of its legal qualification in different public order regimes and in terms of the legality and legitimacy of states' response to this increasingly dangerous phenomenon. In other words, in this legally unarticulated space, there are no resolute answers to the questions when a certain activity on the Internet becomes a means of internal or interstate conflict (*ad bellum*) and which rules should apply in that case (*in bello*). In addition, the instrumentalization of the Internet for influence, pressure and coercion over states can be carried out in ways that evade the regulation of traditional international legal regimes. In covert and visible hybrid wars, the Internet is becoming a means of warfare, and international law is being abused to justify it.

On the other hand, it can be reasoned that the existing international law has risen to this challenge. Namely, the Internet could just be considered as one new area of communication in which relations that are already regulated by international law are manifested. The problem of uncertain legal qualification of cyber violence, due to the possibility of being placed under different regimes of public order – is not new either, because it can be pointed out for other violent activities as well. Thus, for example, murder in peacetime is treated in war as a permissible method of warfare or as a war crime, if it is committed in violation of humanitarian law. New technological achievements are happening everyday anyway, so it may be more advisable to interpret existing law progressively and broadly by applying analogies, filling legal gaps, and consulting legal and other experts.

The answer to the question – how it should further go – should respect the reality of contemporary competitive and conflicting international relations, but it is more important to affirm basic ethical values on which international law is based. In this sense, a solution should be chosen that is in the function of strengthening the foundations of international law, i.e. peaceful coexistence and sovereign equality of states. This approach indicates that we should opt for progressive development in this area and the establishment of international cyber law, by adopting and concluding international agreements that would provide adequate responses to the dangers of cyber violence.

The fact that there is no universally accepted interpretation of existing international law that can be applied to the Internet also speaks in favour of the necessity of adopting and concluding of cyber international agreements. The Tallinn Book is a praiseworthy attempt to express *lex lata* and a reliable consultant to legal practitioners, but this unofficial document made under the auspices of a regional military-political alliance does not express the views of legal experts from a number of developing countries. Some of them are leaders in the technological development and use of Internet because of truly unique ability of Internet to provide equal access to all, by destroying dominant notions of someone's intellectual, economic, political, military or other superiority.

Finally, in addition to universal norms, international law needs universal institutions on this issue. Under the auspices of the UN, there are already a number of specialized agencies, which represent forums for international cooperation on important global issues, such as the World Health Organization or the International Atomic Energy Agency. Following their example, a universally established international institution should therefore be a central place for systematizing knowledge about the Internet, formulating legal standards for its use, international cooperation and control.

Starting from the ethical and legal premises that the restriction of war is the beginning of peace (Volzer, 2010: 40) and that the legal contribution to the achievement of this noble goal consists in the criminal prosecution of war criminals (Kelsen, 1944: 102-112), the treaties proposed here would trace two paths of progressive development of international cyber law. These are the pacification of the Internet and the criminalization of cyber violence. The fiths one would consist in the demilitarization of this new area of communication and in strengthening of international cooperation, analogous to the legal regimes agreed for space or the Earth's poles. A good start to that path would be to ban and control the use of certain means and methods of warfare by using Internet, such as legal regimes already established for chemical and nuclear weapons. The second path would be to prescribe international criminal offenses that would sanction the abuse of Internet against sovereignty of states in the Rome Statute of the International Criminal Tribunal.

5. Conclusion

Placed in the context of contemporary hybrid and legal warfare, cyber violence is changing the perception of contemporary international relations. Instead of the idea of global peace spoiled by exceptions in the form of local and regional armed conflicts, a vision of a global hybrid war is emerging in which

covert or visible Internet-mediated violence, alone or in combination with other military and non-military means and methods of warfare, plays an increasingly destructive role.

Applicable international law can be applied analogously to this new area of communication, but there are no universal norms and institutions that would enable the harmonization of different approaches and traditions to the problems of cyber violations. Particular and regional initiatives are certainly useful, but also insufficient to formulate a unified global approach to this problem that knows no national borders. The problem is all the more difficult due to the instrumentalization of international law, which is increasingly used as a means of confrontation instead of as a means of resolving disputes between the states. Therefore, there is a certain danger that the function of international law will become meaningless to the extent that the legal regulation of war will turn into war with law.

Cyber violation is becoming increasingly socially dangerous and calls into question the adequacy of applicable international legal norms. That is why the pacification of the Internet and the criminalization of cyber violence with the instruments of international legal contracting are proposed. If this does not happen, the risk of cyber violation will soon harm not only international legal entities and the international community, but also international law, should be taken seriously.

Literature

- Carlson, J., Yeomans, N. (1975) Whither Goeth the Law – Humanity and Barbarity. U: Smith, M. & Crossley, D. (ur.) The Way Out – Radical Alternatives in Australia. Melbourne: Landsdowne Press, pp. 5.
- Dabović, D. (2007) Globalizacija prava. Beograd: Pravni fakultet i Službeni glasnik.
- Dunlap, C. J. Jr. (2002) Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. Humanitarian Challenges in Military Interventions Conference. Washington D.C: Kennedy School of Government, Harvard University.
- Edlinger, K. (2016) Typology and categorization of armed conflicts under IHL. U: Marchand, C. & Beruto, G. L. (ur.) The Distinction between International and Non-International Armed Conflicts: Challenges for IHL?. Sanremo: The International Institute of Humanitarian Law & Franco Angeli, pp. 39-45.
- Geers, K. (2010) Cyber Weapons Convention. Computer Law & Security Review, 26(5), pp. 547-551, https://doi.org/10.1016/j.clsr.2010.07.005.
- Gervais, M. (2012) Cyber Attacks and Laws of War. Berkeley Journal of International Law, 30(2), pp. 525-579, doi: 10.15779/Z38R66C.

- Henckaerts, J-M., Doswald-Beck, L. (2005) Običajno međunarodno humanitarno pravo. Cambridge: Cambridge University Press, https://doi.org/10.1017/CBO9780511804700.
- ICRC (2013) Handbook of International Rules Governing Military Operations. Geneva: ICRC.
- Kelsen, H. (1944) Peace through Law. Chapel Hill: The University of North Carolina Press.
- Libicki, M. C. (2009) Cyberdeterrence and Cyberwar. Santa Monica: RAND.
- Mosquera, A. B. M., Bachmann, S. D. (2016) Lawfare in Hybrid Wars: The 21st Century Warfare. Journal of International Humanitarian Legal Studies, 7(1), pp. 63–87, https://doi.org/10.1163/18781527-00701008.
- Rašević, Ž. (2017) OTP 1-04 Pravna podrška operacijama. Sarajevo: Zajednički štab Oružanih snaga BiH.
- Rašević, Ž., Vlajnić, J. (2020) Kriminalizacija agresije u savremenom međunarodnom pravu. U: Simović, M. (ur.) Krivično zakonodavstvo i prevencija kriminaliteta. Trebinje: Srpsko udruženje za međunarodnopravnu teoriju i praksu i Ministarstvo pravde RS.
- Roscini, M. (2014) Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, doi:10.1093/acprof:oso/9780199655014.001.0001.
- Sanders, C. M. (2018) The Battlefield of Tomorrow, Today: Can a Cyber Attack Ever Rise to an "Act of War?". Utah Law Review, 2018(2).
- Schmitt, M. N. (2017) Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, https://doi.org/10.1017/9781316822524.
- Schmitt, M. N., Garraway, C., Dinstein, Y. (2006) The Manual on the Law of Non-International Armed Conflict. Sanremo: International Institute of Humanitarian Law.
- Spalević, Ž., Ilić, M. (2017) The Use of Dark Web for the Purpose of Illegal Activity Spreading. Ekonomika, 63(1), doi:10.5937/ekonomika1701073S.
- Tikk, E., Kaska K., Vihul, L. (2010) International Cyber Incidents: Legal Considerations. Talinn: CCDCOE.
- Volzer, M. (2010) Pravedni i nepravedni ratovi. Belgrade: Službeni glasnik.
- Wither, J. K. (2020) Defining Hybrid Warfare. Per Concordiam: Journal of European Security and Defense Issues, 10(1), pp. 7-9.

Other sources:

- Council of Europe (2001) Convention on Cybercrime.
- Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

– ICRC (1949) Geneva Conventions.
– ICRC (1977) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II).
– UN (2000) Convention against Transnational Organized Crime.
– UN General Assembly (2001) GA Res. 56/83: The Articles on State Responsibility UN Doc. A/RES/ 56/83, 12 December 2001.

Online sources:
– Kharpal, A. (2020, May 7th) New cybersecurity report says China-based group is hacking Asia-Pacific governments, CNBC, available at: https://www.cnbc.com/2020/05/07/chinese-hacking-group-naikon-reportedly-spyingon-asia-governments.html accessed on 05.06.2020.
– Live Cyber Threat Map, available at: https://threatmap.checkpoint.com/ accessed on 04.06.2020.
– Sanger, D. E., Perlroth, N. (2019, June 15th) U.S. Escalates Online Attacks on Russia's Power Grid, The New York Times, available at: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html accessed on 05.06.2020.