UDC: 341.123.043:004.738.5
DOI: 10.5937/PDSC25352M

MSc Darija Marković, PhD candidate
Law Institute, RUDN University, Moscow, Russia
email: darija.dm.markovic@gmail.com

JUSTICE IN CYBER CONFLICTS: THE ROLE OF THE UN SECURITY COUNCIL IN ENSURING ACCOUNTABILITY FOR VIOLATIONS OF IHL

Abstract:

Given their ability to seriously threaten the civilian population and vital infrastructure, cyber-attacks pose an increasing threat to global security. Although international humanitarian law (IHL) offers a basis for protecting civilians and limiting conflict, its applicability in cyberspace remains insufficiently defined. This paper explores the function of the United Nations Security Council (UNSC) in guaranteeing accountability for violations of IHL in cyber operations. Through a qualitative analysis of the institutional and legal tools that the UN Security Council can use (resolutions, sanctions, *ad hoc* court procedures, etc.), as well as an examination of relevant incidents of cyber-attacks with serious humanitarian implications, the paper highlights important issues, including those on jurisdiction, sovereignty and political limitations in the application of international law. The goal of the paper is to review the possibilities of the Security Council, in cooperation with other UN bodies, to overcome these challenges, to ensure effective attribution of responsibility for cyber incidents and thereby improve the international system of protection and justice for victims. The paper concludes that such opportunities not only exist, but also that strengthening the authority of the Security Council has a very important role in building a fair mechanism for determining responsibility in cyber conflicts, with the aim of protecting IHL standards and ensuring justice for victims.

Keywords: *international law, cyber security, attribution of responsibility, UN mechanisms, civil infrastructure*

1. INTRODUCTION

In contemporary international relations cyber space appears more and more frequently as a new area of conflict where legal norms, technical capabilities and political ambitions enter into a complex interplay. Of particular concern are cases in which cyber-attacks produce consequences that go beyond the scope of technical destabilization and enter the realm of serious humanitarian consequences: disruption of hospital operations, sabotage of energy infrastructure, or targeted destruction of communication systems during tensions or in armed conflict. In this context, one question arises: can the United Nations Security Council (UNSC) act as an institutional guarantor of international humanitarian law (IHL) in the digital sphere, and if yes, then how?

The aim of this paper is to examine the capacities, legal mechanisms and political limitations of the UN Security Council in determining responsibility for cyber-attacks

that produce humanitarian consequences. Starting from the basic norms of international law and relying on the analysis of institutional practices and available documentation (resolutions, reports of working groups, judicial practice, etc.), the paper uses a qualitative methodology of analysis of normative and institutional documents, focusing on cases that have precedent or illustrative character.

From the analytical point of view, the work tries to show how the formal structure of responsibility, which implies decision-making in the UN Security Council based on Chapter VII of the UN Charter, is increasingly giving way to informal institutional channels, regional initiatives and the so-called convergent practices. Although such responses often seem fragmented and legally non-binding, their increasing frequency and normative orientation point to the potential of building a new regime of international responsibility in the cyber domain.

Structurally, the work consists of three sections, with introductory and final part. The second section discusses the normative framework of international humanitarian law in the context of cyber operations, with special reference to the problem of demarcation between permitted and prohibited use of cyber means according to the rules of armed conflict. The third section analyses the institutional capacity and political limitations of the UN Security Council as a potential guarantor of accountability. The fourth section is focused on alternative institutional mechanisms and pragmatic responses that occur outside the formal scope of the UN Security Council yet can contribute to the protection of the civilian population in the digital context. The conclusion synthesizes the findings and returns them to the normative horizon of protection and justice.

2. IHL IN CYBER CONTEXT: NORMS AT THE INTERSECTION OF PHYSICAL AND DIGITAL

International humanitarian law (IHL), as a legal framework that governs behaviour during armed conflicts, is based on a number of fundamental principles: distinction, proportionality, military necessity, humanity, prohibition of unnecessary suffering and limitation of means and methods of warfare. These principles, although developed in the context of conventional conflicts, have universal weight – they apply to all forms of warfare, including those that take place in cyberspace.[1]

The principle of distinction requires that a clear distinction be made at all times between military objectives and civilian objects. In the digital domain, that boundary is often blurred: infrastructure, such as electricity distribution, hospitals or communication networks, has a dual function. An attack on such systems, even when directed at military facilities, can produce disproportionate damage to civilians.[2]

1 ICRC. (2023, March 7). *Towards common understandings: the application of established IHL principles to cyber operations*. (2025, June 5) Retrieved from: https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/

2 Farid, F. S. (2023–2024). The principles of distinction and proportionality in international humanitarian law. *Hull Law Review*, *1*, 9–14, pp. 9–11. Retrieved from: https://www.hlr.wordpress.hull.ac.uk/wp-content/uploads/2024/09/Hull-Law-Review-Vol-1-2023-24-Farah-Principles-of-Distinction-and-Proportionality.pdf

Proportionality dictates that attacks whose expected civilian losses are disproportionate to the expected military advantage be avoided. In cyber operations, however, predicting the consequences is difficult: a digital attack on the energy system can cause chain effects – from shutting down hospitals to jeopardizing water supplies – further complicating the assessment of proportionality.[3]

Military necessity permits the use of only those means necessary to achieve a legitimate military objective. However, even when an attack is technically feasible and militarily useful, it must be consistent with humanitarian constraints. This principle cannot be used as a justification for measures prohibited by other rules of IHL.[4]

Humanity and the prohibition of unnecessary suffering further limit the use of means that cause excessive or unavoidable suffering, even when directed against legitimate military objectives. In the cyber context, this could include, for example, attacks that cause long-term psychological consequences for civilians, or that prevent access to basic services such as healthcare.[5]

Tallinn Manual 2.0, as the most comprehensive attempt to systematize international law in the cyber domain, confirms that IHL applies to cyber operations during armed conflicts. However, the expert group that worked on this document acknowledges that many questions remain open – including when a cyber-attack meets the threshold of an "attack" in the sense of IHL, and how damage is assessed in the digital environment.[6]

In practice, digital operations targeting civilian infrastructure show that the line between cyber incidents and actions that produce effects comparable to armed conflicts is becoming increasingly blurred. Cyber-attacks on systems vital to health, safety, and dignity of civilians – such as hospitals, water supplies, or energy grids – can create consequences that are humanitarian in nature, even in the absence of physical force. Nevertheless, the international legal community has not developed a unified response to this type of jeopardy: it remains uncertain whether such operations meet the threshold of application of international humanitarian law, and the mechanisms for attributing responsibility remain fragmented and operationally weak.[7],[8]

Thus, although IHL formally covers cyber operations that take place in the context of armed conflicts, its application in the digital space remains based on interpretation, without a solid institutional support that would enable consistent application and sanctioning of violations.

3 *Ibid*, pp. 11—13.

4 ICRC. (2022). *The Principles of Humanity and Necessity*. (2025, June 5) Retrieved from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf

5 United Nations. (2021). *Group of Governmental Experts on Advancing responsible state behaviour in cyberspace in the context of international security: Note by the Secretary-General (A/76/135)*. General Assembly, 76th session. (2025, June 5) Retrieved from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

6 Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

7 ICRC, 2023, *op. cit*.

8 United Nations, 2021, *op. cit.*

3. UN SECURITY COUNCIL: INSTITUTIONAL POTENTIAL AND POLITICAL LIMITATIONS

The UN Security Council, as a body primarily responsible for preservation of international peace and security, has formal competences that, even theoretically, could include cyber-attacks with serious humanitarian consequences. The UN Charter[9] anticipates the possibility of reacting in cases of "threats to the peace, violations of the peace and acts of aggression" (Article 39) and in such situations reaction could include political statements, economic sanctions, and even the use of force (Article 42). However, cyberspace and its specific dynamics raise a number of questions regarding the practical applicability of these mechanisms.

Formally, the UN Security Council is not excluded from acting in the digital domain. Nothing in the UN Charter limits its jurisdiction to physical areas or conventional weapons. In theory, a massive cyber-attack that paralyzes the health care system, disables critical infrastructure networks, or produces prolonged insecurity for the civilian population could qualify as a "threat to the peace" and thereby trigger Chapter VII mechanisms. However, in practice, the UN Security Council's responses to such incidents have been lacking – not only due to normative vagueness, but also due to deep political divisions within the body itself.

As the previous attempts to formalize digital security within the UN have shown, the issue of cyber conflict is rapidly transitioning from legal to geopolitical level. The permanent members of the UN Security Council, who have the right of veto, are also some of the main actors in the cyber domain, which further relativizes the possibility of joint action. There is no consensus even on the definition of a cyber-attack that would require a collective response, let alone on the specific measures that the UNSC could undertake in order to determine responsibility, which further complicates the institutional application of international law norms pertaining to the digital domain.[10]

In a formal sense, the UN Security Council has the capacity to adopt binding resolutions, establish investigative mechanisms, introduce targeted sanctions and, in exceptional cases, support the establishment of ad hoc tribunals. However, its effectiveness in this domain in practice depends primarily on the political will of the permanent members, and not on legal powers. Without minimal political consensus, institutional potential remains unused, and so responsibility for cyber-attacks with humanitarian consequences continues to be displaced from the domain of justice and float somewhere between technical attribution and political silence.

9 United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. (2025, June 7) Retrieved from: https://www.un.org/en/about-us/un-charter/full-text

10 Madubuike-Ekwe, J. N. (2021). *Cyberattack and the Use of Force in International Law*. *Beijing Law Review*, *12*, 631–649, pp. 634–637. (2025, June 7) Retrieved from: https://www.scirp.org/journal/paperinformation.aspx?paperid=109577

4. ALTERNATIVE APPROACHES AND PRAGMATISM OF INSTITUTIONAL RESPONSIBILITY

Under the circumstances where the UN Security Council is demonstrating a limited ability to act in the event of serious cyber incidents, alternative institutional and normative models for interpretation and application of the rules of international humanitarian law are increasingly attracting attention. Instead of a formal threshold for a collective reaction, partial responses that combine elements of a legal, political and technical approach appear often more and more.[11]

One type of such development is relying on specialized agencies and mechanisms within the UN system, such as UNIDIR, or the ICRC, which do not have the binding force of UN Security Council decisions, but contribute to building normative clarity through the so-called "law through practice". By expressing their positions on the principles of distinction, proportionality, protection of the civil infrastructure and attribution of conduct in cyberspace, these actors form an expert consensus that becomes relevant even in the absence of political unity.

The second direction is represented by initiatives coming from the states themselves and regional organizations – such as the "Paris Call for Trust and Security in Cyberspace"[12] or the OSCE's trust-building measures.[13] Although they lack legal binding, they allow for a somewhat coordinated action and serve as platforms through which different expectations regarding responsibility in cyberspace are articulated. In this sense, they are more of an indicator of will than an instrument of action, but it is precisely therein that their potential lies.

In the third, pragmatic layer, an increasing role is played by transnational professional networks, which, though not introducing norms, provide infrastructure for rapid recognition, attribution and response to digital incidents with humanitarian implications.[14] They function below the threshold of formal responsibility, but can have a significant influence on the behaviour of states through reputational mechanisms.

To summarize, the absence of a centralized response does not mean the absence of institutional dynamics. On the contrary, the fragmentation of mechanisms opens up space for normative adaptation in which relevance comes not only from legal obligation, but also from convergent practice.[15] Although this does not guarantee the protection of victims in

11 Pytlak, A., & Lad, S. (2024, August 8). *Strengthening Global Cyber Resilience Through UN Security Council Initiatives: Paving the way for the United Nations Security Council to uphold global cyber peace and security*. Stimson Center, Emerging Tech Program. (2025, June 10) Retrieved from: https://www.stimson.org/2024/strengthening-global-cyber-resilience-through-un-security-council-initiatives/

12 République française. (2018). *Paris Call for Trust and Security in Cyberspace*. Ministry for Europe and Foreign Affairs. (2025, June 10) Retrieved from: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf

13 OSCE. (2016). *Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs)*. Permanent Council, PC.DEC/1202. (2025, June 10) Retrieved from: https://www.osce.org/pc/227281

14 Brannon, R. B. (2014). *Cyber Security Studies at the Marshall Center. per Concordiam*, George C. Marshall European Center for Security Studies. (2025, June 10) retrieved from: https://perconcordiam.com/cyber-security-studies/

15 Convergent practice means a process in which different international actors – especially states and expert institutions – develop similar patterns of behavior, normative attitudes or operational approaches in

the moment of crisis, it at least allows building foundations for more responsible behaviour of actors – and provides instruments to open space in the digital domain for future legal regulation, instead of waiting for its late arrival.

5. CONCLUSION

In the absence of a clear institutional response and formal international consensus, the legal regime for the use of force in cyberspace remains fragmented – both conceptually and operationally. The boundary between the use of cyber means as a hostile act, use of force and armed attack still depends on interpretive models, while concepts such as distinction, proportionality, special protection and even neutrality suffer the burden of technical indeterminacy. In such a landscape, the UN Security Council has been acting less and less as the final interpretive authority, while a number of parallel practices has been appearing more and more – from regional initiatives and "calls for trust", to professional networks with reputational capacity and informal modes of cooperation.

What appears to be a weakness in the international legal sense – absence of formal obligation, diffusion of actors, normative flexibility – in the political-operational sense can represent exactly what enables institutional adaptation and response in real time. This, paradoxically, creates a space in which emerging law is not the result of an elite agreement, but the result of the cumulative practice of actors who have not formally agreed, but act, speak and react similarly enough to ultimately shape the expected standard of behaviour.

Therefore, instead of looking for an unequivocal answer that will not come, perhaps we should take seriously exactly what seems transitional, temporary, and even informal. In cyberspace, law is written less and assumed more. Precisely because of this, any effort toward institutional accountability, however fragmented, remains important not because of the structures themselves, but because of those who these structures must protect: civilians.

a certain area, although without a formal agreement or binding instrument. Such practice does not produce law in the technical sense, but it can contribute to shaping the expected standards of behavior and guide the interpretation of existing norms. *See:* Green, A. (2021). *The Precarious Rationality of International Law: Critiquing the International Rule of Recognition*. *German Law Journal*, *22*(8), 1613–1634, pp. 1615–1617. (2025, June 10) Retrieved from: https://www.cambridge.org/core/journals/german-law-journal/article/precarious-rationality-of-international-law-critiquing-the-international-rule-of-recognition/A6BB982F76A98C9366B91F63AC2250B7

Mr Darija Marković, doktorand
Pravni institut Univerziteta RUDN, Moskva, Rusija
email: darija.dm.markovic@gmail.com

PRAVDA U SAJBER SUKOBIMA: ULOGA SAVETA BEZBEDNOSTI UN U OBEZBEĐIVANJU ODGOVORNOSTI ZA KRŠENJA MHP

Apstrakt:

S obzirom na njihovu sposobnost da ozbiljno ugroze civilno stanovništvo i vitalnu infrastrukturu, sajber napadi predstavljaju sve veću pretnju svetskoj bezbednosti. Iako međunarodno humanitarno pravo (MHP) nudi osnovu za zaštitu civila i ograničavanje sukoba, njegova primenljivost u sajber prostoru ostaje nedovoljno definisana. U ovom radu se istražuje funkcija Saveta bezbednosti Ujedinjenih nacija (SB UN) u garantovanju odgovornosti za kršenja MHP u sajber operacijama. Kvalitativnom analizom institucionalnih i pravnih alata koje Savet bezbednosti UN može da koristi (rezolucije, sankcije, *ad hoc* sudske procedure i dr.), kao i ispitivanjem relevantnih incidenata sajber napada sa ozbiljnim humanitarnim implikacijama, u radu se ističu važna pitanja, uključujući ona o nadležnostima, suverenitetu i političkim ograničenjima u primeni međunarodnog prava. Cilj rada je da sagleda mogućnosti Saveta bezbednosti, uz saradnju sa drugim telima UN, za prevazilaženje ovih izazova, radi obezbeđenja efikasnog pripisivanja odgovornosti za sajber incidente i time poboljšanja međunarodnog sistema zaštite i ostvarivanja pravde za žrtve. U radu se zaključuje da takve mogućnosti ne samo da postoje, već i da jačanje autoriteta Saveta bezbednosti ima veoma važnu ulogu u izgradnji pravednog mehanizma utvrđivanja odgovornosti u sajber sukobima, a u cilju zaštite standarda MHP i obezbeđivanja pravde za žrtve.

Ključne reči: *međunarodno pravo, sajber bezbednost, pripisivanje odgovornosti, UN mehanizmi, civilna infrastruktura*

6. REFERENCES

1. Brannon, R. B. (2014). *Cyber Security Studies at the Marshall Center*. *per Concordiam*, George C. Marshall European Center for Security Studies. (2025, June 10) retrieved from: https://perconcordiam.com/cyber-security-studies/
2. Farid, F. S. (2023–2024). The principles of distinction and proportionality in international humanitarian law. *Hull Law Review*, *1*, 9–14, pp. 9–11. Retrieved from: https://www.hlr.wordpress.hull.ac.uk/wp-content/uploads/2024/09/Hull-Law-Review-Vol-1-2023-24-Farah-Principles-of-Distinction-and-Proportionality.pdf
3. ICRC. (2022). *The Principles of Humanity and Necessity*. (2025, June 5) Retrieved from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/02_humanity_and_necessity-0.pdf
4. ICRC. (2023, March 7). *Towards common understandings: the application of established*

IHL principles to cyber operations. (2025, June 5) Retrieved from: https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/

5. Madubuike-Ekwe, J. N. (2021). *Cyberattack and the Use of Force in International Law*. *Beijing Law Review*, *12*, 631–649, pp. 634–637. (2025, June 7) Retrieved from: https://www.scirp.org/journal/paperinformation.aspx?paperid=109577
6. OSCE. (2016). *Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (ICTs)*. Permanent Council, PC.DEC/1202. (2025, June 10) Retrieved from: https://www.osce.org/pc/227281
7. Pytlak, A., & Lad, S. (2024, August 8). *Strengthening Global Cyber Resilience Through UN Security Council Initiatives: Paving the way for the United Nations Security Council to uphold global cyber peace and security*. Stimson Center, Emerging Tech Program. (2025, June 10) Retrieved from: https://www.stimson.org/2024/strengthening-global-cyber-resilience-through-un-security-council-initiatives/
8. République française. (2018). *Paris Call for Trust and Security in Cyberspace*. Ministry for Europe and Foreign Affairs. (2025, June 10) Retrieved from: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf
9. Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
10. United Nations. (1945). *Charter of the United Nations and Statute of the International Court of Justice*. (2025, June 7) Retrieved from: https://www.un.org/en/about-us/un-charter/full-text
11. United Nations. (2021). *Group of Governmental Experts on Advancing responsible state behaviour in cyberspace in the context of international security: Note by the Secretary-General (A/76/135)*. General Assembly, 76th session. (2025, June 5) Retrieved from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf