Review science paper

UDK 004.056.5:351.749(100) DOI 10.7251/DEFEN2556083R COBISS.RS-ID 142987521

LEGAL REGIME OF STATE JURISDICTION IN CYBERSPACE: INTERNATIONAL LEGAL FRAMEWORK FOR ATTRIBUTION OF RESPONSIBILITY FOR TRANSNATIONAL CYBER OPERATIONS

Mitar Radonjić[1]
Milica Župljanić[2]
Ivan Ćorović[3]

Abstract: The expansion of cyberspace represents one of the most complex challenges of contemporary international law, particularly in the context of determining state jurisdiction and attribution of responsibility for transnational cyber operations. This paper analyzes the existing international legal framework for establishing state jurisdiction in the cyber domain, examines legal standards for attribution of cyber attacks to states and considers the evolution of international legal norms in this area. Through comparative analysis of state practice, judicial decisions and international documents, the paper identifies key legal gaps and proposes directions for future normative regulation. The research shows that traditional principles of territorial and personal jurisdiction require significant adaptation for effective application in cyberspace, while standards for attribution of responsibility remain unclear and controversial. The paper concludes that a comprehensive international legal instrument is needed that would clearly define jurisdictional frameworks and attribution criteria in the cyber domain.

Keywords: cyber jurisdiction, attribution of responsibility, international law, cyber operations, state responsibility, cyber warfare

1 fakultet.tutin@live.com
2 fakultet.tutin@live.com
3 fakultet.tutin@live.com

1. INTRODUCTION

The digital revolution of the last decade has fundamentally changed the nature of international relations and posed new, unexpected challenges to international law. Cyberspace, as a virtual domain that transcends traditional geographical boundaries, has called into question the basic postulates of the Westphalian system of state sovereignty and jurisdiction (Schmitt, 2017). Transnational cyber operations, which can be executed from any point in the world and directed against targets in other states, require a reexamination of classic principles of international law and the establishment of new legal frameworks. The problem of jurisdiction in cyberspace is particularly complex because traditional territorial principles, on which the Westphalian system of international law is based, are not directly applicable to virtual operations that can be executed through servers and networks in different jurisdictions (Buchan, 2018). Additionally, the issue of attribution - that is, determining which state or non-state actors are behind certain cyber operations - represents a technical and legal challenge without precedent in traditional international law. The relevance of this research stems from the growing number of cyber incidents that have significant political, economic and security consequences. From attacks on Estonian infrastructure in 2007, through the Stuxnet virus that targeted Iranian nuclear facilities, to recent ransomware attacks on critical infrastructure, cyber operations have become an integral part of contemporary international relations (Tikk *et al*., 2010). However, the legal response to these challenges remains fragmented and inconsistent. This paper aims to analyze the existing international legal framework for establishing state jurisdiction in cyberspace and critically assess standards for attribution of responsibility for transnational cyber operations. The research will through three key aspects - theoretical foundations of jurisdiction, practical challenges of attribution and evolution of legal norms - provide a comprehensive overview of the current state and directions of future development of this area of international law.

2. THEORETICAL FOUNDATIONS OF STATE JURISDICTION IN CYBERSPACE

International law traditionally recognizes five basic principles for establishing state jurisdiction: territorial, personal (active and passive), protective and universal principle (Brownlie, 2008). In the context of cyber operations, each of these principles faces significant adaptation challenges. The territorial principle, as the most widely accepted basis of jurisdiction, is based on the physical location of the event or action. In cyberspace, however, the concept of "place" becomes problematic when operations are executed through servers in different states, use proxy servers to mask location or rely on cloud computing infrastructure (Svantesson, 2013). The case Estonia v. Russia (2007) illustrates this problem - while attacks targeted Estonian infrastructure, their origin was difficult to establish due to the use of botnets distributed worldwide.

The personal principle, which is based on the nationality of the perpetrator or victim, also requires modification in the cyber context. The active personal principle allows a state to exercise jurisdiction over its nationals regardless of the place of commission of the act, which is particularly relevant for cyber operations that can be executed from any location (Ryngaert, 2015). However, establishing the identity and nationality of cyber actors is often technically and practically impossible. A significant contribution to the theoretical foundation was made by the International Court of Justice in the case Nicaragua v. United States (1986), establishing that states have an obligation not to allow the use of their territory for attacks on other states. This principle, known as the "due diligence" obligation, takes on a new dimension in cyberspace where states must take reasonable measures to prevent the use of their cyber infrastructure for attacks on third countries (Schmitt, 2017).

The concept of virtual territoriality represents an attempt to adapt the territorial principle to cyberspace through the establishment of legal fictions that connect cyber activities with physical territories (Johnson & Post, 1996). This approach suggests that every cyber act has an "effect" on a certain territory, enabling the application of traditional jurisdictional principles. State practice shows different approaches to this issue. The United States applies a broad interpretation of territorial jurisdiction, con-

sidering that it has the right to jurisdiction over cyber operations that "pass through" American infrastructure or have an "effect" on American territory (Brenner, 2007). The European Union, on the other hand, is developing an approach based on "substantial connection" between the cyber operation and the territory of the state. Critical analysis shows that virtual territoriality, while practically useful, can lead to conflicts of jurisdiction and legal uncertainty. The problem of "spillover" effects - when a cyber operation has consequences in multiple states - requires a coordinated international response and clear criteria for determining primary jurisdiction (Buchan, 2018).

3. ATTRIBUTION OF RESPONSIBILITY IN TRANSNATIONAL CYBER OPERATIONS

Attribution of cyber operations to states represents one of the most complex aspects of international cyber law (Knežević, 2015; Knežević, 2017). International law of state responsibility, codified in Articles on State Responsibility (ILC, 2001), establishes clear criteria for attribution: the action must be performed by a state organ or persons acting in the capacity of a state organ, or the state must have effective control over the non-state actor. In the cyber context, the application of these criteria is problematic for several reasons. First, cyber operations are often executed by specialized non-state groups or individual hackers who may, but do not have to be, connected with the state apparatus (Roscini, 2014). Second, the technical complexity of cyber attacks allows the use of "false flag" operations where responsibility is attempted to be attributed to third parties.

A significant precedent is the case Georgia v. Russia (2008), where cyber attacks on Georgian infrastructure during the war were executed by non-state groups that, according to Georgian claims, were supported by Russia (Knežević, 2025). The International Court of Justice has not yet made a final decision on the attribution of these attacks, which illustrates the complexity of the problem. The "effective control" test, established in the case Nicaragua v. United States, requires that the state have operational control over specific acts of non-state actors (ICJ, 1986). In the cyber domain, this test is difficult to apply because a state can provide logistical support to hacker groups without direct control over their operations (Schmitt, 2017).

Legal standards for attribution must be supported by adequate evidentiary requirements. In traditional international law, evidence is usually physical in nature and can be independently verified. Cyber evidence, however, is digital, can easily be falsified or destroyed, and requires specialized technical knowledge for interpretation (Rid & Buchanan, 2015). Development of international standards for cyber forensics represents a key challenge. The NATO Cooperative Cyber Defence Centre of Excellence developed the Tallinn Manual as an attempt to codify international law applicable to cyber warfare, but this document does not have binding legal force (Schmitt, 2013). The Manual suggests that technical attribution must be supplemented by legal analysis that takes into account all relevant circumstances (Knežević, 2024). State practice shows different approaches to evidentiary standards. The United States often relies on intelligence sources that are not publicly available, which makes international verification of attribution difficult (Eichensehr, 2017). The European Union insists on more transparent procedures and coordination with international partners.

The complexity of cyber attribution has led to the development of the concept of collective attribution, where multiple states or international organizations jointly assess responsibility for certain cyber operations (Eichensehr, 2017). This approach can increase the credibility of attribution and reduce the possibility of political instrumentalization. An example of collective attribution is the joint statement by the EU, NATO and partners on Russia's responsibility for the NotPetya ransomware attack in 2017. Although this attribution did not have direct legal consequences, it represents an important precedent for coordinated international response (EU Council, 2018). International cooperation in cyber attribution faces challenges related to intelligence information sharing, different legal systems and political sensitivities. The Budapest Convention on Cybercrime represents the most comprehensive legal framework for international cooperation, but focuses on criminal acts rather than state cyber operations (Council of Europe, 2001).

4. EVOLUTION OF INTERNATIONAL LEGAL NORMS IN THE CYBER DOMAIN

The current international legal framework for cyber operations is based on the application of existing norms of international law to the new technological environment. The United Nations Charter, the Inter-

national Covenant on Civil and Political Rights, international humanitarian law and customary international law form the basis of this framework (Schmitt, 2017). Article 2(4) of the UN Charter, which prohibits the threat or use of force in international relations, applies to cyber operations that reach the level of "armed aggression". However, defining the threshold for this classification remains controversial. The Tallinn Manual suggests that cyber operations that cause physical damage or casualties can be considered use of force, but this interpretation is not universally accepted (Schmitt, 2013). The right to self-defense, established by Article 51 of the UN Charter, also applies to cyber attacks that reach the level of "armed aggression". The Estonia case (2007) raises the question of whether DDoS attacks that paralyze national infrastructure can justify self-defense, including kinetic retaliation. International humanitarian law applies to cyber operations during armed conflicts, requiring respect for the principles of distinction, proportionality and precaution (Dinstein, 2012). Cyber attacks on civilian objects are prohibited, but the classification of "dual-use" infrastructure (such as electrical grids) remains problematic (Vejnović & Knežević, 2024).

In the absence of a comprehensive multilateral framework, states are developing regional and bilateral agreements to regulate cyber issues. The European Union adopted the Directive on Security of Network and Information Systems (NIS Directive) which establishes minimum standards for cyber security among members (EU, 2016). NATO has through Article 5 of the North Atlantic Treaty extended the concepts of collective defense to the cyber domain, although the practical implementation of this policy is still undefined (NATO, 2016). The Shanghai Cooperation Organization has developed an alternative approach that emphasizes information security and sovereignty in cyberspace (SCO, 2011). Bilateral agreements between major powers, such as US-China agreements on banning cyber espionage in the commercial sector, represent a pragmatic approach to specific problems (White House, 2015). However, these agreements are often politically motivated and have limited legal force.

The need for a comprehensive international legal instrument for cyberspace is becoming increasingly obvious. Proposals include a new convention under the auspices of the UN, expansion of existing agreements or development of "soft law" instruments through the Group of

Governmental Experts (GGE) or Open-ended Working Group (OEWG) (UN, 2021). Main challenges for achieving consensus include different concepts of cyber sovereignty, disagreements about the definition of cyber attack, and geopolitical tensions between major actors. Western countries advocate an open, free cyberspace based on the rule of law, while authoritarian regimes insist on state control and information sovereignty (Mueller, 2017). A hybrid approach that combines binding norms for the most serious cyber threats with soft law instruments for operational standards perhaps represents the most realistic option. This approach would enable gradual harmonization of national legislation and establishment of minimum international standards.

5. PRACTICAL CHALLENGES OF IMPLEMENTING JURISDICTIONAL FRAMEWORKS IN CYBERSPACE

The implementation of theoretical frameworks of state jurisdiction in the practical context of cyber operations faces a series of complex problems that require a multidisciplinary approach combining legal, technological and political elements. State practice over the last fifteen years reveals a significant gap between normative expectations and operational capabilities when it comes to exercising jurisdiction over cyber incidents that transcend national boundaries. One of the most significant practical challenges is the problem of synchronizing national legislation that regulates cybercrime and cyber security. Analysis of existing legal systems shows that definitions of basic concepts such as "unauthorized access", "computer sabotage", or "cyber espionage" differ significantly among states, which complicates international cooperation in investigation and prosecution of cross-border cyber incidents (Simović, Vejnović & Knežević, 2024). For example, what one state classifies as "hacking" another may consider legitimate penetration testing or security vulnerability research, which creates legal uncertainty for international actors operating in cyberspace.

The problem is further complicated by the fact that cyber operations often involve "live evidence" that can be altered, deleted or moved during the investigation. Unlike traditional crimes where physical evidence usually retains its integrity during the investigative process, digital evidence requires specialized procedures for preservation, analysis and presenta-

tion before judicial bodies. This specificity requires not only harmonization of substantive norms but also alignment of procedural standards among different jurisdictions. International practice shows that states have developed different approaches to the problem of multi-jurisdictional cyber incidents. The United States applies an aggressive approach to extraterritorial jurisdiction, often invoking the "effects doctrine" when cyber operations have consequences on American territory, regardless of server location or actor nationality. This approach is illustrated in the case United States v. Bout (2011), where American authorities extended their jurisdiction to cyber activities that had "reasonably foreseeable effects" on American interests. The European Union, on the other hand, is developing an approach based on "significant connection" that requires a substantial link between the cyber operation and the territory of the state that wants to exercise jurisdiction (Knežević, 2024).

Technological development represents a continuous challenge for legal practice, as traditional mechanisms for identifying location - such as IP addresses - are becoming increasingly unreliable due to the use of VPN networks, Tor browsers, and distributed cloud computing systems. The practice of "jurisdiction shopping" where cybercriminals consciously choose jurisdictions with weaker legislation or limited cooperation capabilities further complicates the problem. This phenomenon is particularly pronounced in the case of ransomware operations that are often executed from countries that do not extradite their nationals or have limited cooperation with victim countries. The financial aspect of cyber operations represents an additional dimension of jurisdictional challenges. Modern cyber operations often involve complex financial flows that pass through multiple jurisdictions, using cryptocurrencies, online payment platforms, and offshore financial centers. Tracking and freezing assets related to cybercrime requires coordination between different legal systems with different standards for financial forensics and international legal assistance. The Colonial Pipeline ransomware attack case (2021) illustrates these challenges - while it was possible to track the flow of bitcoins used for ransom payment, practical recovery of funds required coordination between American, British and several other jurisdictions.

The role of the private sector in exercising de facto jurisdiction in cyberspace represents another unexplored aspect of practical implemen-

tation (Vejnović & Knežević, 2025). Large technology companies such as Google, Microsoft, Facebook and Amazon control a significant part of cyber infrastructure and often have greater technical capabilities for identification, tracking and interruption of cyber operations than many state agencies. This reality raises fundamental questions about the delegation of traditionally state functions to private actors and the need for regulation of their activities in the context of state jurisdiction. The practice of "active defense" and "hack back" operations performed by private companies further complicates jurisdictional issues. When an American company responds to a cyber attack originating from another country by accessing hacker servers in a third country, the question arises which state has the right to regulate this activity and by what criteria. Current law does not provide clear answers to these situations that are becoming increasingly common in practice.

Procedural aspects of international legal assistance in cyber cases show additional practical problems. Traditional mechanisms such as mutual legal assistance (MLA requests) are often too slow for the cyber context where evidence can be deleted in the time needed for formal communication between states. Development of expedited procedures for cyber cases becomes imperative, but requires careful balancing between speed of response and protection of sovereignty and human rights. The capacity of smaller states to effectively exercise jurisdiction in cyberspace represents a significant challenge for global cyber security. Many developing countries do not have the technical, financial or human resources needed for investigation of sophisticated cyber operations, which creates "security havens" that can be exploited by cybercriminals. International organizations such as ITU, UNODC and Interpol are developing capacity building programs, but these efforts are still insufficient in relation to the scope of the problem.

Cultural and linguistic factors also play a significant role in practical implementation of jurisdictional frameworks. Cyber operations often involve social engineering and techniques that are specific to certain cultures and languages, which requires culturally sensitive analysis of evidence and international cooperation that respects these differences. Additionally, different understandings of privacy, state security and freedom of expression among cultures can complicate cooperation in cases that

have political or security implications. The temporal dimension of cyber operations represents an additional practical challenge. Unlike traditional crimes that usually occur within a specific timeframe, cyber operations can be long-lasting, repeated or latent, activating only after a significant time period. This characteristic complicates the application of statutes of limitations and other time restrictions in different legal systems, especially in cases that require coordination between multiple jurisdictions with different timeframes for criminal prosecution.

6. JUDICIAL PRACTICE AND PRECEDENTS IN CYBER JURISDICTION

The development of judicial practice in the field of cyber jurisdiction represents a critical factor for understanding the practical application of theoretical frameworks of international law in the digital domain. Analysis of key judicial decisions at national and international levels reveals the gradual shaping of new legal standards that seek to respond to the unique challenges that cyber operations pose to traditional concepts of jurisdiction and state responsibility. The pioneering case in this area is Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme (2000), where the French court established jurisdiction over an American company due to content that was available to French users via the internet. This decision set an important precedent for the "targeting" principle that allows states to exercise jurisdiction over foreign actors whose content or activities target their nationals. However, the attempt to implement this decision in the American legal system resulted in a conflict of jurisdictions and raised questions about the limits of extraterritorial exercise of jurisdiction in cyberspace.

A significant contribution to the development of cyber jurisdiction was made by the European Court of Human Rights in the case Delfi AS v. Estonia (2015), where the court considered the responsibility of online platforms for user content in the context of freedom of expression. The court established that online platforms can bear responsibility for content published by users if they do not take reasonable measures for moderation, which had far-reaching consequences for understanding jurisdictional obligations in cyberspace. This case also demonstrated how traditional human rights apply in the digital context and how national courts

can exercise jurisdiction over activities that take place in cyberspace. American judicial practice has developed a specific approach to cyber jurisdiction through a series of landmark decisions. In the case United States v. Gorshkov (2001), the federal court established that American authorities have jurisdiction to investigate cyber attacks that target American victims, even when executed from abroad. The court applied the principle of "effects doctrine" arguing that cyber operations that have effects on American territory fall under American jurisdiction regardless of the physical location of the perpetrator. This approach was further developed in the case United States v. Ivanov (2000), where the court extended jurisdiction to a Russian national who from Russia executed cyber attacks on American companies.

European judicial practice shows a more cautious approach to extraterritorial jurisdiction in cyber cases. The case Glawischnig-Piesczek v. Facebook (2019) before the Court of Justice of the European Union sets important principles for jurisdiction over multinational tech companies. The court established that national courts can order the removal of illegal content from global platforms, but only within the limits of their territorial jurisdiction. This decision attempts to balance national jurisdiction with the practicalities of the global internet and sets limits on the extraterritorial application of national laws. International arbitration practice also contributes to the development of cyber jurisdiction. The case Yukos v. Russia (2014) before the Permanent Court of Arbitration in The Hague, although not directly a cyber case, established important principles for determining state responsibility for activities performed through complex corporate structures that may be relevant for cyber operations executed through proxy organizations or non-state actors.

The practice of national courts in cybercrime cases reveals different approaches to the problem of multi-jurisdictional cyber operations. The German Bundesgerichtshof in case BGH 1 StR 266/18 (2018) established that jurisdiction can be established based on server location even when users and administrators are in different countries. This approach gives significance to physical infrastructure in determining jurisdiction, which is in contrast to approaches that focus on effects or targeting.

British judicial practice, particularly through cases before the High Court of Justice, has developed a sophisticated approach to cyber juris-

diction that combines traditional common law principles with the specificities of the digital environment. The case Soriano v. Forensic News LLC (2021) illustrates how British courts apply the "forum conveniens" test in cyber cases, considering factors such as server location, linguistic availability of content and target audience.

Asian legal systems show unique approaches to cyber jurisdiction that reflect different cultural and legal traditions. The Japanese Supreme Court in cases related to cyber mobbing (2017) established that jurisdiction can be based on the victim's location regardless of the perpetrator's location, which represents an extension of the traditional passive personal principle. The Singapore Court of Appeal in the case Ng Kek Wee v. Sim City Technology Ltd (2014) developed a "real and substantial connection" test for cyber cases that requires a significant connection between the dispute and jurisdiction.

The practice of international criminal courts, although limited in the area of cybercrime, provides important insights into the application of international law to digital activities (Knežević & Martinović, 2024). The International Criminal Court in its preliminary rulings has considered how cyber operations can fit into existing definitions of war crimes and crimes against humanity, which has implications for jurisdiction in cases of cyber warfare. Administrative and regulatory proceedings also contribute to the development of cyber jurisdiction. The European Commission through its data protection decisions, particularly in implementing GDPR, establishes precedents for the extraterritorial application of European standards to non-European companies. The case Google Spain SL v. Agencia Española de Protección de Datos (2014) established the "right to be forgotten" principle that has global implications for cyber jurisdiction and demonstrates how administrative bodies can effectively exercise jurisdiction in cyberspace.

The developmental trend in judicial practice shows a gradual shift from strictly territorial approaches to more flexible frameworks that take into account the realities of the global internet. However, this evolution is not uniform and different legal systems continue to develop divergent approaches, which creates legal uncertainty for international actors. The need for harmonization of judicial practice (Martinović, 2025) through international instruments or model legislation is becoming increasingly

obvious as a way to resolve these inconsistencies. Future development of judicial practice in cyber jurisdiction will likely be shaped by the growing number of cases that involve new technologies such as artificial intelligence, IoT devices and blockchain technology. These technologies pose additional challenges to traditional concepts of jurisdiction and require further evolution of legal standards.

7. CONCLUSION

The analysis of the legal regime of state jurisdiction in cyberspace and the international legal framework for attribution of responsibility for transnational cyber operations reveals fundamental challenges that the digital era poses to traditional international law. The research shows that existing legal frameworks, developed for physical territories and conventional security threats, require significant adaptation for effective application in the virtual domain. The territorial principle of jurisdiction, as the cornerstone of the Westphalian system, shows its limitations in cyberspace where the concept of "place" becomes a fluid and often indeterminate category. Virtual territoriality, as an attempt to bridge this gap, provides a partial solution but simultaneously generates new problems of overlapping jurisdictions and legal uncertainty. The personal principle, although conceptually applicable, faces practical obstacles of identification and verification of cyber actors' identities. Attribution of responsibility for cyber operations represents perhaps the most complex aspect of this issue. The existing "effective control" test from the Nicaragua case is difficult to apply to the cyber domain where non-state actors can operate with varying degrees of autonomy from state sponsors. The need for new evidentiary standards and procedures for technical attribution becomes imperative for credible application of international law in cyberspace. The evolution of international legal norms in the cyber domain shows a fragmented approach without clear consensus on fundamental principles. Regional and bilateral agreements provide partial solutions but cannot replace the need for a comprehensive multilateral framework. Geopolitical divisions over the concept of cyber sovereignty further complicate achieving international consensus. For future developments in this area, it is crucial to establish a hybrid legal framework that combines adaptation of existing norms of international law with the development of specific instruments for the cyber domain. This

framework must include clear criteria for establishing jurisdiction in cyberspace, standardized procedures for attribution of cyber operations and mechanisms for international cooperation in investigation and prosecution of cyber incidents. Finally, the international community must recognize that cyberspace is not a "legal vacuum" but a domain where existing international law applies with the need for specific adaptations. Only through a coordinated international approach that balances technological realities with legal principles is it possible to establish a stable and predictable legal regime for cyberspace that will serve the interests of an increasingly digitalized international community.

8. REFERENCES

1. Brenner, S. W. (2007). *Law in an era of "smart" technology*. Oxford University Press.
2. Brownlie, I. (2008). *Principles of public international law* (7th ed.). Oxford University Press.
3. Buchan, R. (2018). Cyber attacks: Unlawful uses of force or prohibited interventions? *Journal of Conflict and Security Law*, 17(2), 212-227.
4. Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
5. Dinstein, Y. (2012). Cyber war and international law: Concluding remarks at the 2012 Naval War College International Law Conference. *International Law Studies*, 89, 276-285.
6. Eichensehr, K. E. (2017). The cyber-law of nations. *Georgetown Law Journal*, 103(2), 317-380.
7. EU Council. (2018). *Declaration by the High Representative on behalf of the EU on malicious cyber activities*. Press release 133/18.
8. European Union. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1.
9. International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America). ICJ Reports 1986.

10. International Law Commission. (2001). *Articles on Responsibility of States for Internationally Wrongful Acts*. UN Doc. A/56/10.
11. Johnson, D. R. & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 48(5), 1367-1402.
12. Knežević, S. (2015). *Rat po mjeri Pentagona: Građanski rat u Siriji i Iraku*. Narodna biblioteka „Ivo Andrić".
13. Knežević, S. (2017). *Kako su srušili Jugoslaviju: Od 14-og kongresa SKJ do proglašenja nezavisnosti Kosova*. Udruženje građana za književnu i publicističku djelatnost „Slovo".
14. Knežević, S. (2024). *Prauzrok: nacrt za uvod u morfologiju kosmologije, evolucije i teogonije*. Metaphysica.
15. Knežević, S. (2024). *The High Representative and the Constitutional Crisis in Bosnia and Herzegovina*. Svarog, 15(28), 139-161. http://dx.doi.org/10.7251/SVR2428139K
16. Knežević, S. (2025). Krivičnopravna zaštita ustavnog poredka SFRJ. *Godišnjak Pravnog fakulteta Univerziteta u Banjoj Luci*, 46(46), 103-128, DOI https://doi.org/10.63356/gpf.2024.006
17. Knežević, S. (2025). *Imperijalna prenapregnutost Sjedinjenih Američkih Država i Specijalna vojna operacija u Ukrajini*. Banja Luka: Evropski defendologija centar.
18. Knežević, S. (2025). Dekodiranje genocidne namjere: pravna evolucija dokaznih standarda u digitalnoj eri. *Godišnjak Fakulteta pravnih nauka*, 267-286.
19. Martinović, T. (2025) *Sport Diplomacy and Security Challenges during the Cold War*. Defendologija, br. 55, 151-166.
20. Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.
21. NATO. (2016). *Warsaw Summit Communiqué*. Press Release 100/16.
22. Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2), 4-37.
23. Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press.
24. Ryngaert, C. (2015). *Jurisdiction in international law* (2nd ed.). Oxford University Press.

25. Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
26. Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
27. Shanghai Cooperation Organization. (2011). *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*.
28. Simović, M., Vejnović, D. & Knežević, S. (2025). Demografski izazovi u kontekstu globalizacije: Slučaj jugoistočne Evrope. *Demografske i etničke promjene u Bosni i Hercegovini od 2013. do 2024. godine*, 69-97.
29. Svantesson, D. J. (2013). *Private international law and the internet* (3rd ed.). Kluwer Law International.
30. Tikk, E., Kaska, K. & Vihul, L. (2010). *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence.
31. United Nations. (2021). *Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*. UN Doc. A/76/135.
32. Vejnović, D. & Knežević, S. (2024). Hegemonija u unipolarnom svijetu: izazovi i posljedice za međunarodno pravo. Bezbjednost zemalja regiona u svjetlu nove bezbjednosne arhitekture, 7-30.
33. Vejnović, D. & Knežević, S. (2025). Primjena digitalne forenzike u otkrivanju cyber kriminala. Savremeni izazovi i prijetnje bezbijednosti, Fakultet bezbjednosnih nauka Univerziteta u Banjoj Luci, 422-442.
34. White House. (2015). *Fact Sheet: President Xi Jinping's State Visit to the United States*. Office of the Press Secretary.

Paper received: 15.5.2025.
Paper approved: 30.6.2025.