Ekonomická univerzita v Bratislave

Fakulta medzinárodných vzťahov

Ekonomické, politické a právne otázky medzinárodných vzťahov 2025

Zborník z medzinárodnej vedeckej konferencie

konanej 29. – 30. mája 2025

Economic, political and legal Issues of international relations 2025

Proceedings of an International Scientific

Conference held May 29 - 30, 2025

Lacušová, Sabina, Ing.
Taliian, Iryna, Ing.
Vlková, Eva, Mgr.

Authors are responsible for the content of their papers.

Publisher: *Vydavateľstvo EKONÓM, 2025*

Is published once a year.

ISBN 978-80-225-5233-2
ISSN 2585-9404

Contents

CYBERSECURITY AS A KEY ELEMENT IN INTERNATIONAL RELATIONS[1]

Halyna Hyryavets[a] – **Rastislav Kazanský**[b] – **Lucia Rýsová**[c]

[a] Faculty of Political Sciecne and International Relations, Matej Bel University in Banská Bystrica, Kuzmányho 1, 974 01 Banská Bystrica, Slovak Republic, e-mail: halyna.hyryavets@student.umb.sk
[b] Faculty of Political Sciecne and International Relations, Matej Bel University in Banská Bystrica, Kuzmányho 1, 974 01 Banská Bystrica, Slovak Republic, e-mail: rastislav.kazansky@umb.sk
[c] Faculty of Political Sciecne and International Relations, Matej Bel University in Banská Bystrica, Kuzmányho 1, 974 01 Banská Bystrica, Slovak Republic, lucia.rysova@umb.sk

Abstract: This article analyses the growing importance of cybersecurity within contemporary international relations. It focuses on cyber threats as a novel challenge to state sovereignty and emphasizes the need to integrate cybersecurity into global security strategies. The study applies a descriptive-analytical method, historical-comparative analysis, and case studies of recent cyberattacks. Particular attention is paid to the legal vacuum in cyberspace and the lack of universally accepted international norms. The findings confirm that cybersecurity is a fundamental component of both national and collective security, requiring a comprehensive, coordinated, and multilateral approach.
Keywords: Cybersecurity, International Law, Cyber Threats, Cyberspace
JEL: K33, K24, F51

Introduction

In recent decades, the field of international security has undergone a profound transformation. Whereas in the past, security was primarily understood as the protection of the state from military threats posed by other states, today's security environment is significantly more complex and includes new dimensions—one of the most prominent being cyberspace. Cyberspace can no longer be perceived solely as a technological or infrastructural category; rather, it has become a geopolitical and strategic domain in which an increasing number of hostile activities are concentrated.

Cybersecurity has become increasingly relevant within the broader context of security studies. It now stands as one of the fundamental pillars supporting national sovereignty, political stability, and the overall functionality of the modern state. Unlike in the past, today's environment requires states to protect not only their territory, population, and military forces, but also their digital infrastructure. Any disruption in this domain can lead to tangible consequences comparable to those caused by conventional attacks. The specific nature of cyber threats, marked by anonymity, asymmetry, global scope, and the potential for rapid escalation, presents distinct and complex challenges for international law, defence structures, and diplomatic engagement.

A fundamental problem remains the absence of universally accepted norms governing state behaviour in cyberspace. Unlike traditional military conflicts, which are subject to the rules of international humanitarian law, cyber operations often occupy a grey zone between peace and war, between attack and espionage, and between state and non-state actors. Cyberspace, therefore, not only introduces new threats but also raises critical questions about how to ensure its stability, transparency, and predictability.

[1] This article was published with the support of the KEGA 020UMB-4/2025: Theory of Conflicts in International Relations – Structural and Cultural Causes. A compendium of educational materials for university and joint degree programmes.

This article focuses on examining cybersecurity as an increasingly important element of international security. It defines the key concepts associated with cyberspace, discusses the historical context of its militarization, and maps current trends in cyberattacks, with a particular emphasis on developments in 2025. Special attention is paid to the interplay between technological advancement, strategic state behaviour, and efforts to establish a functional framework for global cyber governance. The objective is to demonstrate that without adequately integrating cybersecurity into international structures, sustainable security in the 21st century cannot be achieved.

1 Definition of Terms

Compared to previous periods, international security — understood as the mutual security of states — has taken on a new dimension. States, as traditional subjects of international law, now bear the additional responsibility of safeguarding their security not only in inter-state relations but also against phenomena and threats closely linked to technological and scientific progress. Negative activities in cyberspace, involving a wide range of actors, are a clear example.

In recent years, we have increasingly witnessed a shift in the domain of operations, the "ammunition" used, and the intended targets. The migration of numerous activities into cyberspace exemplifies this transformation. Some experts even warn that certain cyber operations signal the reality of an ongoing cyber war — perceived only by those not living in the "illusion of peace."[2]

Historically, humanity operated in two physical domains — land and sea. Later, with technological advancement, airspace and outer space were added. Today, we recognize a fifth domain: cyberspace. Unlike the others, cyberspace has a global character, blurs national boundaries, transcends political systems, and is populated by a diverse range of actors — from individuals and groups to states.[3]

Threats no longer emanate solely from states or criminal and terrorist organizations, but increasingly from hackers or ideologically motivated individuals ("hacktivists"). Cyber technologies and skills are relatively easy and cheap to acquire, enabling even weak states or non-state actors to inflict significant damage on powerful conventional military forces. The financial aspect is one of the key advantages of cyber threats—some authors claim a cyber warfare campaign could be conducted for the price of replacing tank treads, making it an attractive option for states.[4]

Consequently, the position of individual states is increasingly challenged. This is exacerbated by the interconnected nature of emerging threats, particularly hybrid threats — those combining political, military, economic, social, and informational tools, often involving both state and non-state actors. These threats frequently disrupt state functions, necessitating stronger international cooperation — predicated, however, on suitable political conditions. [5]

As in the physical world, the "cyber world" is subject to security threats including hacking, DDoS attacks, data theft, terrorist or extremist exploitation of the internet, psychological operations, and cyber espionage. These activities show that cyberspace is not immune to danger, a fact increasingly reflected in state security strategies. However, not every cyber operation qualifies as a cyberattack. According to Rule 30 of the Tallinn Manual, a cyberattack is "a cyber operation, whether offensive or defensive, that is reasonably expected

[2] VAN PUYVELDE, D. (2019): Cybersecurity: Politics, governance and conflict in cyberspace, p. 145.
[3] VALUCH, J. (2022): Armed conflicts and cyber threats as challenges for international law in the 21st centry, p. 98.
[4] LEVICKÝ, D. (2024): Kybernetická bezpečnosť a jej aplikácie, p. 38.
[5] AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE (2019): *Aktuálne výzvy kybernetickej bezpečnosti* (v podmienkach bezpečnostných zložiek) – zborník príspevkov z vedeckej konferencie, p. 8.

to cause injury or death to persons or damage or destruction to objects." This definition is significant because the term "attack" carries specific legal restrictions in the law of armed conflict—such as the protection of civilians and civilian infrastructure. This also applies in cyberspace, as affirmed by the Tallinn Manual. [6]

The Manual refers to Article 49(1) of the First Additional Protocol to the Geneva Conventions, which defines an attack as "acts of violence against the adversary, whether in offense or defense." The determining factor is the violent consequence of the act. Non-violent cyber operations — such as psychological operations or espionage — do not qualify as cyberattacks but rather cybercrime or cyber threats. Given our dependency on digital infrastructure, ensuring cybersecurity is now a fundamental precondition for state functioning and service delivery. In a world of rapid technological advancement, "absolute security" remains an illusion. Nevertheless, international cooperation brings us closer to this ideal.[7]

The growing number of cyber operations affecting the security of states, institutions, and individuals has made "cybersecurity" an increasingly relevant concept. In cyberspace, not only states but also non-state actors and individuals play active roles. Cybersecurity is generally understood as the ability to defend against malicious activity in the digital domain. It is now an integral component of national security strategies. Cyberattacks can disrupt national security, endanger sovereignty, and threaten state functions and public services. Thus, cybersecurity has become a key factor in maintaining state stability.

Though cyberspace lacks physical borders, its protection primarily falls under national jurisdiction. A comprehensive approach to cybersecurity involves effective strategies and security measures covering a wide range of threats; a clear legislative framework defining institutional responsibilities during cyber incidents; and precise national-level competencies to ensure effective response and foster international cooperation.

Cyber threats can originate from various sources and manifest as disruptive activities targeting individuals, critical infrastructure, public and private institutions, or national governments. Their main characteristics include transnationality, ambiguity, decentralization, anonymity of actors, low entry costs, and the capacity to strike from a distance without physical presence—all of which give these threats long-term potential.

Cyber threats frequently transcend borders and blur the lines between public and private, military and civilian spheres. Traditional geographic boundaries, historically fundamental to national sovereignty, lose relevance in cyberspace. As a result, national security is increasingly dependent on international cooperation. One of the most crucial concepts in the current security landscape is "cyberspace." International legal scholars' understanding of this domain is shaped by how various spaces are treated under international law.

The term "cyberspace" was first used by W. F. Gibson in his 1982 short story *Burning Chrome* and later in his 1984 novel *Neuromancer*. Since then, the term has gained global traction amid the relentless expansion of digital networks. Cyberspace has evolved into a distinct communication network with a unique status, not entirely subject to any one country, legal system, or jurisdiction. In the digital age, the assertion by philosopher Karl Jaspers — that one cannot be heard in public while remaining unseen — no longer holds. On the internet, users can be both heard and hidden simultaneously.[8]

Other scholars define cyberspace as a globally interconnected network of digital information and communication infrastructures, including the internet, telecommunications systems, computer networks, and embedded information systems. According to the 2006 U.S.

[6] AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE (2020): *Aktuálne výzvy kybernetickej bezpečnosti*: *Special edition 2020* – zborník príspevkov, p. 4.
[7] SCHMITT, M. N. et al. (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, p. 56.
[8] KOLOUCH, J. (2019): CyberSecurity, p. 40.

National Military Strategy, cyberspace is a domain defined using electronic and electromagnetic spectrum to store, modify, and exchange data across networks and associated physical infrastructures.[9]

Security institutions, including armed forces, treat cyberspace as a battlefield. The U.S. Department of Defence defines it as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." Alongside land, sea, air, and space, cyberspace is now recognized as the fifth domain of warfare. Unlike traditional domains, however, it is man-made and lacks fixed boundaries.[10]

IT experts assert that absolute security in cyberspace is unattainable. Historically, control over physical domains required material superiority — dominance at sea, for instance, required a powerful navy. In cyberspace, superiority depends not on numbers, but on technological capabilities, knowledge, and access to information. Human behaviour and user interaction play an essential role.[11]

Cybersecurity depends not only on technological tools but also on social dimensions — such as user behaviour and their ability (or failure) to respond to cyber threats. According to the *Tallinn Manual 2.0*, cyberspace consists of three layers: physical, logical, and social. The physical layer includes tangible components like cables, routers, servers, and computers. The logical layer comprises the interconnections and protocols that facilitate data exchange. The social layer encompasses the individuals and groups engaged in cyber activities.[12]

2 The Development of Cybersecurity in Historical Perspective

In recent years, the topic of cybersecurity has received growing attention both due to global security threats and in connection with specific incidents. Cybersecurity has been evolving for approximately forty years, constantly adapting and advancing alongside the development of modern technologies.[13]

The origins of cybersecurity can be traced back to the 1970s, during the time of ARPANET, the predecessor of the modern internet. Early models of malicious software and principles for protecting information systems were not described until decades later. In 1983, Fred Cohen introduced a program capable of replicating itself across systems by concealing itself within a regular application. This marked the beginning of the era of computer malware. The first malware infection affecting a larger number of computers was identified in 1988, impacting around ten percent of all systems connected to ARPANET. In the United States during the 1980s, there was a significant increase in high-profile attacks targeting national laboratories and private companies. The year 1983 also saw the first known use of a Trojan horse virus. In 1987, the first commercial antivirus software was introduced, although there are differing opinions regarding its original developer. That same year, programmers Andreas Lining and Kai Figge released antivirus software for the Atari ST, which became known as the Ultimate Virus Killer.[14]

Slovak programmers were also active in this field during the same period. In 1987, Peter Paško and Miroslav Trnka developed a program designed to detect the first computer virus

[9] VALUCH, J. (2022): Armed conflicts and cyber threats as challenges for international law in the 21st century, p. 103.
[10] VAN PUYVELDE, D. (2019): Cybersecurity: Politics, governance and conflict in cyberspace, p. 54.
[11] U.S. DEPARTMENT OF DEFENSE (2018): Joint Publication 3-12: Cyberspace Operations, p. 6.
[12] SCHMITT, M. N. et al. (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, p. 14.
[13] LEVICKÝ, D. (2019): Úvod do kybernetickej bezpečnosti, p. 15.
[14] SINGER, P. W. (2014): Cybersecurity and Cyberwar: What Everyone Needs to Know, p. 82.

within an information system. At that time, they had no idea that they would later become leading figures in Slovakia's antivirus software market. Their program was named NOD, which stood for "Nemocnica na okraji disku" (Hospital on the Edge of the Disk), inspired by a popular television series in former Czechoslovakia.[15]

The field of cybersecurity began to develop more intensively in the second half of the twentieth century as the internet and digital technologies expanded. The first cyber incidents typically involved individuals attempting to access or disrupt computer systems. In more recent decades, however, cyber operations have increasingly become instruments of geopolitical competition.

One of the first widely known state-sponsored cyberattacks occurred at the beginning of the twenty-first century. Among the most notable incidents was the Stuxnet attack targeting Iran's nuclear facilities. This operation has been attributed to the United States and Israel. Since then, cyber campaigns have become a standard feature of geopolitical confrontation, frequently targeting governments, financial institutions, and critical infrastructure.[16]

Stuxnet was a computer worm discovered in 2010, although it was likely developed several years earlier. It caused real physical damage to industrial systems. The worm specifically targeted SCADA systems produced by Siemens, which controlled various industrial processes. In this case, the malware attacked uranium enrichment centrifuges at Iran's Natanz nuclear facility. Of approximately 45,000 infected systems, around sixty percent were located in Iran, strongly suggesting that Iran was the primary target. Similar infections were later identified in Indonesia and India.

Experts have noted that the complexity of Stuxnet indicates it was a government project with a military purpose. Most sources attribute its development to the United States and Israel. In 2011, other variants of similar malware were discovered, including DuQu, which has been referred to as Stuxnet 2.0. Unlike the original, DuQu was intended for espionage and the theft of intellectual property from industrial control systems. It also attempted to compromise certification authorities.

Stuxnet was the first known example of a cyber weapon specifically designed to cause physical damage to another country's infrastructure. It was most likely developed by democratic governments and established a new precedent in the domain of cyber warfare.[17]

3 Cyberattacks in 2025

Although the year 2025 is far from over, and we are currently only in its first half (May 2025), it is already evident that this is an exceptionally dynamic period in the field of cybersecurity. From the perspective of international relations, cyberspace is increasingly becoming a central arena of geopolitical confrontation, involving the interests of state actors, intelligence services, and non-state entities.

State-sponsored actors, particularly from the People's Republic of China, the Russian Federation, the Democratic People's Republic of Korea, and the Islamic Republic of Iran, remain the primary sources of globally coordinated cyber operations. One of the most significant incidents was the breach of Morocco's National Social Security Fund by hackers linked to Algeria. This attack led to the exposure of personal and financial data of nearly two million individuals from more than 500,000 companies. In the United States, the email accounts of 103 banking regulators at the Office of the Comptroller of the Currency (OCC) were compromised, allowing attackers to access over 150,000 emails containing highly sensitive financial information. The attackers gained access through a compromised administrator account, and their identities have not yet been officially confirmed.

[15] LEVICKÝ, D. (2019): Úvod do kybernetickej bezpečnosti, p. 37.
[16] SINGER, P. W. (2014): Cybersecurity and Cyberwar: What Everyone Needs to Know, p. 104.
[17] VAN PUYVELDE, D. (2019): Cybersecurity: Politics, governance and conflict in cyberspace, p. 60.

Chinese cyber units were detected during U.S. Cyber Command's "hunt forward" operations, which revealed the presence of Chinese malware in the networks of partners in Latin America. In parallel, Chinese actors continued espionage campaigns targeting governmental, telecommunications, and media sectors in Southeast Asia, Hong Kong, and Taiwan. These operations often involved hiding within cloud services such as Dropbox. Within China, reports indicated a wave of foreign cyberattacks, with more than 1,300 incidents targeting fourteen key sectors during 2024 alone.[18]

North Korean cyber operatives expanded their activities into Europe, targeting government and defence entities. They gained access by impersonating remote contractors, which enabled them to collect sensitive data and even blackmail former employers. At the same time, North Korea carried out the largest cryptocurrency theft in history, stealing 1.5 billion USD in Ethereum from the ByBit exchange and laundering at least 160 million USD within 48 hours.

Iranian hacker groups focused on government networks in Iraq and the telecommunications sector in Yemen. They used custom backdoors and unique command-and-control methods. Several attempts were also made to compromise nuclear facilities in Israel, along with continued espionage activities across the Middle East. Across Europe, cyber incidents were often linked to the foreign policy positions of EU member states. In Germany, Russian hackers compromised the email accounts of the ruling Social Democratic Party. Similar intrusions occurred in Poland and the Czech Republic. Romania experienced repeated attacks on its electoral system, and Italy was targeted following a meeting between the Prime Minister and the President of Ukraine.

The United Kingdom faced a significant data breach involving military personnel, with Chinese groups suspected of being behind the attack. In Canada, a disinformation campaign targeted Deputy Prime Minister Chrystia Freeland. In France, a massive data leak from the national health system affected nearly half of the population. Several high-profile incidents demonstrated how cyberattacks are increasingly intertwined with international political narratives. One such case was the public accusation against Russia for disrupting Ukraine’s tax and communication infrastructure, along with the systematic surveillance of Kyiv’s air defence systems through compromised webcams.[19]

These developments clearly show that cybersecurity is no longer merely a technological issue but a critical component of international security and diplomacy. In the current global context, security policy cannot be effectively developed without recognizing the growing impact of cyber threats. Cyberspace has become a strategic arena in which states test their capabilities to protect institutions, citizens, and critical systems.

Cyber operations are no longer limited to wartime activities; they are now a routine element of ongoing geopolitical rivalry. This makes it essential to embed cybersecurity systematically into national security strategies, defence doctrines, and multilateral frameworks such as NATO, the European Union, and the United Nations.[20]

Cybersecurity today represents a new form of national sovereignty. A state’s ability to protect its digital infrastructure, respond to incidents, and resist hybrid threats is becoming one of the key pillars of modern geopolitics. In a world marked by rising tensions and increasing technological interdependence, cyberspace must be recognized not only as the domain of IT experts but also as a political and strategic space of the twenty-first century.

One of the most pressing challenges of the current international system is the absence of universally accepted rules and norms that regulate the behaviour of states and other actors in

[18] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (2025): Significant Cyber Incidents, apríl 2025, p. 5.
[19] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (2025): Significant Cyber Incidents, apríl 2025, p. 4.
[20] RIORDAN, S. (2019): Cyberdiplomacy: Managing security and governance online, p. 126.

cyberspace. While traditional forms of armed conflict are governed by international conventions – such as the Geneva Conventions – and institutional frameworks, cyber operations still occur in a legally diffuse and strategically unbalanced environment.

Although several significant initiatives exist, including the 2001 Budapest Convention on Cybercrime, which remains one of the few multilateral legal instruments in the cyber domain, their scope is mainly focused on criminal law, and they lack universal acceptance. For example, countries such as Russia, China, and several others are not signatories to this agreement.[21]

International organizations such as the United Nations, NATO, and the European Union are actively working to develop frameworks and instruments for the protection of critical infrastructure and the sharing of best practices in cyber defence. However, their effectiveness remains limited due to diverging strategic interests, asymmetry in technological capabilities, and fundamentally different value systems among states.

Another major challenge is the fact that cyberattacks often operate in a grey zone between peace and war. States increasingly use cyber tools for espionage, public opinion manipulation, election interference, or economic weakening of adversaries, all while maintaining plausible deniability. This complicates the attribution of responsibility at the international level and slows down the development and enforcement of binding norms.

The situation is further complicated by the rapid pace of technological development, particularly in areas such as artificial intelligence and quantum computing. These technologies are transforming the nature of potential cyber threats – from algorithm-driven disinformation campaigns to possible attacks on quantum communication networks. States that fail to invest in adapting and developing their own cyber defence capabilities in time may find themselves in a strategically vulnerable position.

As a result, experts increasingly emphasize that the future of cybersecurity will inevitably depend on the quality and scope of international cooperation. Establishing trustworthy and transparent multilateral platforms for incident response, information exchange, terminological alignment, and the adoption of common ethical principles for cyber warfare are key prerequisites for sustainable global stability.[22]

Without such steps, cyberspace risks becoming a lawless domain in which stronger actors can systematically undermine the sovereignty of weaker states without any effective means of defence or international accountability. Ultimately, it becomes evident that cybersecurity is not merely a technical issue but an existential security concern for every state. It must be fully integrated into both national and international security strategies.

Conclusion

The analysis of cyber threat evolution shifts in the security paradigm, and the current level of vulnerability clearly demonstrates that cybersecurity has become an essential component of today's security environment. Given the nature of cyberspace—its global reach, lack of regulation, technological accessibility, and the diversity of actors—cybersecurity represents a fundamental challenge for both national and supranational institutions.

Findings indicate that states which historically dominated through conventional military power no longer hold a guaranteed advantage in the cyber domain. On the contrary, it is increasingly evident that small states and even non-state actors are capable of inflicting significant damage at minimal cost. The asymmetry of cyberattacks, their covert origins, and

[21] SCHMITT, M. N. et al. (2017): Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, p. 31.
[22] EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES (2014): Riding the digital wave: The impact of cyber capacity building on human development, p. 78.

the frequent inability to attribute responsibility undermine traditional concepts of accountability in international law.

The year 2025, even in its first half, has already made it clear that cyber operations have become a routine part of international reality. These operations span espionage, economic disruption, and direct interference in the internal affairs of states. This trend repeatedly confirms that national security strategies must adapt, innovate, and reflect new conditions in which an invisible attack can lead to visible consequences.

A key insight is that national security can no longer be ensured by domestic means alone. Cybersecurity is increasingly becoming a matter of international cooperation, including intelligence sharing, the development of joint defence mechanisms, and the harmonization of legal frameworks. In this context, it is crucial to strengthen the role of international organizations such as the United Nations, NATO, and the European Union, which can serve as platforms for knowledge exchange, negotiation of behavioural norms in cyberspace, development of international standards and laws, and coordination of responses to cyberattacks. In conclusion, this study affirms that cybersecurity is no longer a mere subfield of information security or a technical issue for IT departments. It has become an integral part of state power, national defence, and international politics. Ensuring cybersecurity requires not only technical tools but also political will, a robust legal framework, and binding multilateral commitments. In the twenty-first century, a state that cannot protect its cyberspace will not be able to protect its sovereignty.

References:

1. AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE (2019): *Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek)* – zborník príspevkov z vedeckej konferencie. Bratislava: Akadémia Policajného zboru v Bratislave, 2019. ISBN 978-80-8054-819-3.
2. AKADÉMIA POLICAJNÉHO ZBORU V BRATISLAVE (2020): *Aktuálne výzvy kybernetickej bezpečnosti: Special edition 2020* – zborník príspevkov. Bratislava: Akadémia Policajného zboru v Bratislave, 2020. ISBN 978-80-8054-879-7.
3. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (2024): Significant Cyber Incidents. [online]. In: *CSIS.org*, 2024. [Cited 10. 5. 2025]. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
4. EUROPEAN UNION INSTITUTE FOR SECURITY STUDIES (2014): *Riding the digital wave: The impact of cyber capacity building on human development.* Paris: European Union, Institute for Security Studies, 2014. ISBN 978-92-9198-251-6.
5. KOLOUCH, J. (2019): *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
6. LEVICKÝ, D. (2019): *Úvod do kybernetickej bezpečnosti.* Košice: elfa, s.r.o., 2019. ISBN 978-80-8086-276-3.
7. LEVICKÝ, D. (2024): *Kybernetická bezpečnosť a jej aplikácie.* Košice: Technická univerzita v Košiciach, 2024. ISBN 978-80-553-4022-7.
8. RIORDAN, S. (2019): *Cyberdiplomacy: Managing security and governance online.* Cambridge, Medford: Polity, 2019. ISBN 978-1-5095-3408-1.
9. SCHMITT, M. N. et al. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017.
10. SINGER, P. W. (2014): *Cybersecurity and cyberwar: What everyone needs to know.* New York: Oxford University Press, 2014. ISBN 978-0-19-991811-9.
11. U.S. DEPARTMENT OF DEFENSE (2018): Joint Publication 3-12: Cyberspace Operations. Washington, D.C.: U.S. Department of Defense, 2018.

12. VALUCH, J. (2019): *Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti.* Bratislava: Wolters Kluwer, Univerzita Komenského v Bratislave, 2019. ISBN 978-80-571-0154-3.
13. VALUCH, J. (2022): *Armed conflicts and cyber threats as challenges for international law in the 21st century*. Bratislava: Wolters Kluwer, 2022. ISBN 978-80-571-0552-7.
14. VAN PUYVELDE, D. (2019): *Cybersecurity: Politics, governance and conflict in cyberspace.* Cambridge, Medford: Polity, 2019. ISBN 978-1-5095-2809-7.

Contacts:
Mgr. Halyna Hyryavets
Faculty of Political Science and International Relations
Matej Bel University in Banská Bystrica
Kuzmányho 1
974 01 Banská Bystrica
Slovak Republic
e-mail: halyna.hyryavets@student.umb.sk

doc. PhDr. Rastislav Kazanský, PhD., EMBA
Faculty of Political Science and International Relations
Matej Bel University in Banská Bystrica
Kuzmányho 1
974 01 Banská Bystrica
Slovak Republic
e-mail: rastislav.kazansky@umb.sk

doc. PhDr. Lucia Rýsová, PhD.
Faculty of Political Science and International Relations
Matej Bel University in Banská Bystrica
Kuzmányho 1
974 01 Banská Bystrica
Slovak Republic
e-mail: lucia.rysova@umb.sk

Title: ***Economic, Political and Legal Issues of International Relations 2025***
Proceedings of an International Scientific Conference held on May 29 - 30, 2025

Editors: Ing. Mgr. Olha Brynko, Mgr. Rostyslav Karakash, Ing. Sabina Lacušová, Ing. Iryna Taliian, Mgr. Eva Vlková
Range: 256 pages
Format: Published in an electronic form
Publisher: Vydavateľstvo EKONÓM
Year: 2025
Is published once a year.

ISBN 978-80-225-5233-2
ISSN 2585-9404