

Radoslav Baltezarević*

<https://orcid.org/0000-0001-7162-3510>

Ivana Baltezarević**

<https://orcid.org/0000-0003-4605-1420>

Dragan Nikolić***

<https://orcid.org/0009-0000-0054-6861>

UDC: 341.24:327(100)

341.76:[316.776:07

DOI: 10.5937/MegRev2501151B

Original scientific paper

Received 25.07.2025.

Approved: 15.09.2025.

CYBER THREATS AND DIGITAL DIPLOMACY: COORDINATING STATE RESPONSES WITHIN FRAGMENTED LEGAL FRAMEWORKS****

Abstract: *Digital media have emerged as crucial players in facilitating new forms of interaction, fundamentally changing how we think about diplomacy and national security. The paper explores digital diplomacy, a modern strategy that enables direct communication between state actors, civic society, and diplomats via online channels. Data breaches, online radicalisation, and the challenges of establishing responsibility and legal accountability in cross-border cyberattacks are just a few of the serious issues brought about by the global nature of cyberspace. The issue is made even more complicated by the disjointed legal systems that often struggle to effectively tackle cross-border threats. The paper explores how national laws falter when cyberattacks occur outside of a nation's borders and draws attention to serious flaws in international law. It examines a range of regulation strategies within the context of international norms, including state-driven, self-regulatory, and cooperative models. These include the United States' sector-specific tactics, China's firm position on digital sovereignty, and the EU's emphasis on rights-based digital governance. Additionally, global efforts such as the Budapest Convention and the Tallinn Manual are viewed as important resources for fostering international collaboration. The rising relevance of digital diplomacy is particularly noticeable, especially as we tackle emerging technological hurdles. It's clear that we need stronger diplomatic education, better coordination among countries, and legally sound cooperation mechanisms to effectively tackle cyber threats in our interconnected world.*

Keywords: *Digital Diplomacy, Digital Media, Legal Regulation, International Cooperation*

* Full Professor & Senior Research Fellow, Institute of International Politics and Economics, Belgrade, Republic of Serbia.

E-mail: radoslav@diplomacy.bg.ac.rs

** Research Fellow, Institute for Political Studies, Belgrade, Republic of Serbia.

E-mail: ivana.baltezarevic@ips.ac.rs

*** E-mail: nikolic.dragan.0314@gmail.com

**** The paper presents findings of a study developed as a part of the research project "Serbia and challenges in international relations in 2025", financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2025.

1. INTRODUCTION

Digital media has had a significant influence on new kinds of group interaction.¹ Geographical barriers have become less distinct in terms of group formation and communication due to globalisation and technology advancements. No matter how sophisticated the technology, the new association still suggests that people are at the centre of communication. Both how accurately people can understand the content of a message and how accurately they can understand the emotions included within it can be influenced by the communication channel.²

The use of social media and other digital communication platforms to facilitate contact between diplomats and the general public is known as “digital diplomacy.”³ The primary motivation for the shift of diplomacy to social media was to overcome the constraints of traditional diplomacy and combat online radical recruitment attempts.⁴

Moreover, digital diplomacy refers to the utilisation of the Internet to address foreign policy concerns. Direct communication with prominent people, governments, and civil society is made possible via the Web. Since the Web is frequently used by organisations whose objectives and values diverge from those of diplomats, this is particularly crucial. In these circumstances, it is necessary to discuss and provide opposing views to an internet audience.⁵

National Internet regulation can work when people on a country's territory are recognised as violators of specific norms and Internet activities are clearly specified by current laws. Prosecution under the Criminal Code may be possible for offensive or fraudulent content found on the Internet. Criminal or civil culpability is a consequence of court proceedings where the presence of a criminal offence is established. On the other hand, when the content in question took place outside of a state, national Internet legislation falls flat.⁶

Cybersecurity includes incident prevention, detection, adaptation, and recovery tasks. Intentional or inadvertent, incidents might include anything from

¹ Baltezarević, R. & Baltezarević, B. (2018): “The impact of video games on the formation of esports”, *Facta universitatis Series: Physical Education and Sport*, Vol. 16, No 1. pp. 137-147. DOI: 10.22190/FUPES170614012B

² Byron, K. (2008): “Carrying too heavy a load? The communication and miscommunication of emotion by email”, *Academy of Management Review*, 33(2), 309-327.

³ Lewis, D. (2014): *Digital Diplomacy*, <http://www.gatewayhouse.in/digital-diplomacy-2/> (Accessed: 15.08.2025).

⁴ Pamment, J. (2012): *New public diplomacy in the 21st century: A comparative study of policy and practice*, Oxon, Routledge.

⁵ Holmes, M. (2015): “The future of digital diplomacy”, in Bjola, C, and Holmes, M. (eds), *Digital Diplomacy: Theory and Practice*, New York, Routledge.

⁶ Solum, B. (2009): „Models of Internet Governance“, In Bygrave, L. A., & Bing, J. (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 48-91), Oxford University Press.

unintentional information leaks to identity theft to even meddling in political processes. Each of these can have a wide range of negative impacts on people, groups, and communities.⁷ Teenagers in the technological age deal with a number of security concerns, but privacy and data protection are among the most important ones that lawmakers should address.⁸

The issue of determining the true origin of cyberattacks will not be solved until the best legal strategy for locating and apprehending cyberattack criminals is discovered. The fundamental characteristics of the Internet and cyberspace, which provide users' anonymity and the worldwide scope of their actions, have an impact on this. This is how criminals are able to conceal who they are and where they launch their attacks. States themselves are part of these occurrences, either by participating in such attacks for political purposes or by doing nothing to stop the offenders. The idea that governments are accountable for the deeds of non-state actors is not yet supported by international law, nevertheless. Only when a state either directs or controls non-state actors, or acknowledges or accepts their behaviour as its own, will responsibility be assigned.⁹

Digital diplomacy is becoming increasingly organised, stressing the importance of diplomatic pathways to cultivate a global agreement on norms and collaborative strategies in the realm of cyberspace. This trend shows that we're increasingly aware that traditional legal systems alone aren't enough to tackle the complexities of cross-border cyber threats.¹⁰ To ensure that diplomats can effectively navigate and address digital threats, ranging from AI policy to disputes over internet governance, modern diplomatic education is increasingly incorporating training in technical and cyber skills. A prime example of this is the curriculum introduced by the U.S. State Department in late 2022.¹¹

⁷ European court of auditors (2019): *Challenges to effective EU cybersecurity policy*, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.

⁸ Domazet, S. S. & Šušak Lozanovska, I. (2023): "Dečji podaci i onlajn privatnost - odrastanje u digitalnom dobu", *Politika nacionalne bezbednosti*, 24(1), 153-173. DOI: 10.5937/pnb24-44680

⁹ Global Risks Report (2019): *International law cannot keep up with cyber-criminals*, <https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/>.

¹⁰ Vasiloiu, I.-C. (2023): „Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age“ *Informatica Economica*, Academy of Economic Studies - Bucharest, Romania, Vol. 27(1), 41-50.

¹¹ Geller, E. (2024): *The Tech Crash Course That Trains US Diplomats to Spot Threats*, <https://www.wired.com/story/us-state-department-diplomacy-school/>.

2. LITERATURE REVIEW

The evolution of diplomacy was significantly influenced by the advancement of communication technology and its effects on the dissemination of knowledge.¹² New media has emerged as a result of technological advancements. As more people choose to work, communicate, and get information online, they are continuously exposed to a large number of media messages.¹³ The offline function of the embassy as a middleman is eliminated thanks to digitalisation, which enables direct communication between world leaders and representatives in foreign affairs departments.¹⁴

A fundamentally new “socio-technological” reality is gradually being created as a result of the fourth industrial revolution’s rapid development and the rise of the newest digital technologies. This metaverse will permeate all facets of society and human existence, impacting human consciousness psychology and reality perception.¹⁵ The new diplomatic practice (known as digital diplomacy) can be viewed as a tool that states use to better understand cultures, attitudes, and behaviours; establish and maintain relationships; influence attitudes; and motivate citizens to take actions that should further their interests and values.¹⁶

A nation’s increasing use of social media platforms to accomplish its foreign policy objectives and actively control its reputation and image is sometimes referred to as “digital diplomacy.”¹⁷

People who can confidently solve problems and control their own learning throughout their lives are needed in modern diplomacy. This includes having a strong command of ICT skills, as creativity is now just as vital in education as reading and should be handled as such.¹⁸

It takes a different style of thinking than is typically displayed to cultivate creativity. Educators must be risk-takers in order to adapt new technology creatively.

¹² Hamilton, K. & Langhorne, R. (2011): *The practice of diplomacy: its evolution, theory, and administration*, London, Routledge.

¹³ Baltezarević, I. & Baltezarević, R. (2019): “Prikriveno oglašavanje u novim medijima”, *Baština*, sv. 48, pp. 171-179. DOI: 10.5937/bastina1948171B

¹⁴ Kinne, B.J. (2014): “Dependent diplomacy: signaling, strategy, and prestige in the diplomatic network”, *International Studies Quarterly*, 58:2, 247–259.

¹⁵ Pashentsev, E. N., & Sebekin, S. (2023): “Metaverses, artificial intelligence and challenges to psychological security”, *Politika nacionalne bezbednosti*, (2), 33–37. DOI: 10.5937/pnb25-46760

¹⁶ Melissen, J. (2013): “Public Diplomacy”, in: *The Oxford Handbook of Modern Diplomacy*, 436–452. Oxford, Oxford University Press.

¹⁷ Manor, I. & C. Segev (2015): “America’s Selfie: How The US Portrays Itself On Its Social Media Accounts”, in: Bjola, C. & Holmes, M. (eds): *Digital Diplomacy: Theory and Practice*, New York, Routledge.

¹⁸ Thompson, K. (2016): *Changing the Education Paradigm.... But How?*, <https://fishbowlteaching.com/2016/01/changing-education-paradigm-but-how>.

A professional culture that is centred on routine practice, curriculum, and strict goal-setting will not be beneficial.¹⁹

Since the creation of the Internet, there has been a risk of hacking. Hacking is a significant concern to digital diplomacy since diplomatic operations conducted online are delicate and constantly monitored by the public. For instance, a spear-phishing attack in March 2016 compromised the personal Gmail account of John Podesta, the former White House chief of staff and campaign chairman of US presidential candidate Hillary Clinton. The leak included data from his email, most of which pertained to business-related activities but could be readily shared in correspondence with Clinton. The Russian espionage group Fancy Bear has been blamed for the hack by cybersecurity experts and the US authorities.²⁰

Major disinformation is an issue in areas like the media and the digital environment that are hard to regulate.²¹ From the standpoint of digital diplomacy, the Internet enables people to discuss issues pertaining to both foreign and domestic policy and to participate directly in political activity. Nevertheless, we are also seeing a lot of bad things, from less serious to criminal activity. The lack of complete legal regulation of the Internet and virtual space makes it easier for user harassment, persecution, and human rights abuses to occur. The missing regulation should guarantee the creation of strong foundations that can serve as a solid basis for defining strategies for upholding user privacy, human rights, and human dignity.

The anticipated diplomatic objectives may be significantly diminished by such attacks. A lot of user data is shared online, and when diplomats post information on acts and activities, it can be abused, turned into skewed content, and shared further. Such occurrences show that protective laws are required. Three distinct regulatory models that are characterised by current regulatory methodologies have been found thus far. The first is the state model, also known as the command and control model, in which the state establishes the rules, oversees their application, and penalises those who break them; the second is the self-regulation model, which focuses primarily on the private sector and establishes the rules and carries them out collectively without the involvement of the public; and the third is the cooperative model, which is distinguished by the fact that while the state

¹⁹ Conlon, T. & Simpson, M. (2003): "Silicon Valley versus Silicon Glen: the impact of computers upon teaching and learning: a comparative study", *British Journal of Educational Technology*, 34(2), pp.137-150.

²⁰ Franceschi-Bicchierai, L. (2016): "How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts", *Motherboard*.

²¹ Baltezarević, R. & Baltezarevic, I. (2021): "Daning-Krugerov efekat: Uticaj iskrivljene realnosti na percepciju potrošača prema luksuznim brendovima", *Baština*, Vol. 31 sv. 55, pp. 237-253. DOI: 10.5937/bastina31-33832

maintains initiative and control, the definition of rules, their implementation, and their monitoring of implementation all take place in concert.²²

These regulatory models can be seen all around the world. For example, the EU follows a rights-based and co-regulatory approach, as seen in frameworks like GDPR, NIS2, and the Cybersecurity Act. In contrast, China adopts a state-driven model focused on digital sovereignty, while the U.S. tends to favor regulations that are specific to certain sectors, often working in tandem with the private sector.²³ On top of that, global agreements like the Budapest Convention on Cybercrime and the Tallinn Manual provide legal frameworks for countries to work together on an international level. Yet, the way these treaties are put into action often varies and is complicated by issues of state sovereignty.²⁴

It is possible to identify two areas that practically all nations believe need governmental intervention: the ban on child pornography and the interception of communications between terrorist organisations. However, each nation has a different level of democracy development and human rights respect and preservation. States that neglect respect for human rights provided by international law utilise control to deal with political opponents and organisations that criticise their actions. In such regimes, the state itself may abuse its control over the Internet by blocking websites in an effort to defend human rights and maintain civilian authority over the communications industry. Such legal frameworks may result in repression and overzealous suppression of online communicators. When content is deemed undesirable for social, political, or security reasons, state authorities frequently employ content filtering as the initial technical restriction. When authorities are unable to physically regulate a particular region, filtering is frequently employed. Authoritarian governments have employed this technique to spy on journalists and their sources as well as to keep an eye on and manage dissidents.²⁵

Additionally, political propaganda can be disseminated online. There are now a number of political extremist organisations that spread videos that glorify violence against women, children, people of colour, or political dissidents, or that are flavoured with racism or bigotry. Instructions on how to manufacture explosives

²² Frydman, B., Hennebel, L. & Lewkowicz, G. (2012): "Coregulation and the rule of law." in: Eriksson, J. & Giacomello, G. (2009), Who controls the Internet? Beyond the obstinacy or obsolescence of the State, *International Studies Review*, 11(1), 205-230.

²³ Kapur, A. (2024): *Can the Internet Be Governed?* <https://www.newyorker.com/magazine/2024/02/05/can-the-internet-be-governed?>

²⁴ Radanliev, P. (2024): "Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing", *Journal of Cyber Security Technology*, 9(1), 28-78. DOI: 10.1080/23742917.2024.2312671

²⁵ Eriksson, J. & Giacomello, G. (2009): „Who controls the Internet? Beyond the obstinacy or obsolescence of the State“, *International Studies Review*, 11(1), 205-230.

are even posted on websites.²⁶ Digital diplomacy has transformed from a passive regulatory role to one that involves active negotiation. Countries are joining forces to create standards for digital conduct, participating in initiatives aimed at building trust, and appointing cyber envoys to navigate crises and enhance international relationships.²⁷ In summary, digital diplomacy is a strategic bridge that connects our diplomatic approaches to addressing tech vulnerabilities. It's essential for lowering cyber threats and fostering collaboration on a global scale.²⁸

3. CONCLUSION

The shift in diplomacy brought on by the digital era highlights how essential it is for countries to adapt to the fast changes in technology and the rising cyber threats we encounter. Digital diplomacy opens up new paths for engagement, cooperation, and influence, but it also reveals weaknesses that can jeopardise national security and the stability of international relations. The ongoing absence of standardised legal frameworks is a significant barrier to effective cross-border collaboration, especially in key areas like enforcement, accountability, and attribution.

As states manoeuvre through the complicated landscape of cyber issues, it's evident that the old ways of diplomacy need to change. Digital diplomacy should step up its game, not only by responding to threats, but also by anticipating them through continuous multilateral collaboration and the establishment of widely accepted norms. Legal frameworks need to be flexible while still being firmly rooted in the protection of human rights and the promotion of transparency. It's no longer just a nice-to-have to boost educational and institutional capabilities in cyber skills; it's now an essential component of any state's resilience strategy.

Creating a safe and collaborative digital future means we need to unite and tackle the legal, technical, and political challenges that lie ahead. When executed strategically, digital diplomacy acts as a crucial platform for this coordination. By engaging in inclusive discussions, fostering mutual trust, and aligning our international standards, the global community can effectively manage the challenges and opportunities that the digital era presents.

²⁶ Osce (2004): *Session 2: Online propaganda and the commission of hate crime*, Michael Whine. <https://www.osce.org/cio/33843>.

²⁷ Robinson, R. (2024): *Cyber Diplomacy: A New Frontier in International Relations and Professional Practice*. <https://www.jdsupra.com/legalnews/cyber-diplomacy-a-new-frontier-in-6850511/>.

²⁸ Tokat, Y. (2024): *Cyber Diplomacy: Rethinking Statecraft in the Digital Era*. <https://modern-diplomacy.eu/2024/10/19/cyber-diplomacy-rethinking-statecraft-in-the-digital-era>.

Literature

- Baltezarević, R. & Baltezarević, B. (2018): "The impact of video games on the formation of esports", *Facta universitatis Series: Physical Education and Sport*, Vol. 16, No 1. pp. 137-147. DOI: 10.22190/FUPES170614012B
- Baltezarević, I. & Baltezarević, R. (2019): "Prikriveno oglašavanje u novim medijima", *Baština*, sv. 48, pp. 171-179. DOI: 10.5937/bastina1948171B
- Baltezarević, R. & Baltezarevic, I. (2021). Daning-Krugerov efekat: Uticaj iskrivljene realnosti na percepciju potrošača prema luksuznim brendovima. *Baština*, Vol. 31 sv. 55, pp. 237-253. DOI: 10.5937/bastina31-33832
- Byron, K. (2008): "Carrying too heavy a load? The communication and miscommunication of emotion by email", *Academy of Management Review*, 33(2), 309-327.
- Conlon, T. & Simpson, M. (2003): "Silicon Valley versus Silicon Glen: The impact of computers upon teaching and learning: A comparative study", *British Journal of Educational Technology*, 34(2), pp.137-150.
- Domazet, S. S. & Šušak Lozanovska, I. (2023): "Dečji podaci i onlajn privatnost - odrastanje u digitalnom dobu", *Politika nacionalne bezbednosti*, 24(1), 153-173. DOI: 10.5937/pnb24-44680
- Eriksson, J. & Giacomello, G. (2009): „Who controls the Internet? Beyond the obstinacy or obsolescence of the State“, *International Studies Review*, 11(1), 205-230.
- European court of auditors (2019): *Challenges to effective EU cybersecurity policy*, https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.
- Franceschi-Bicchierai, L. (2016): "How Hackers Broke into John Podesta and Colin Powell's Gmail Accounts", *Motherboard*.
- Frydman, B., Hennebel, L. & Lewkowicz, G. (2012): "Coregulation and the rule of law", in: Eriksson, J. & Giacomello, G. (2009), Who controls the Internet? Beyond the obstinacy or obsolescence of the State, *International Studies Review*, 11(1), 205-230.
- Geller, E. (2024): *The Tech Crash Course That Trains US Diplomats to Spot Threats*, <https://www.wired.com/story/us-state-department-diplomacy-school/>.
- Global Risks Report. (2019): *International law cannot keep up with cyber-criminals*, <https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/>.
- Hamilton, K. & Langhorne, R. (2011): *The practice of diplomacy: Its evolution, theory, and administration*, London, Routledge.
- Holmes, M. (2015): "The future of digital diplomacy", in: Bjola, C, and Holmes, M. (eds), *Digital Diplomacy: Theory and Practice*, New York, Routledge.

- Kapur, A. (2024): *Can the Internet Be Governed?*, <https://www.newyorker.com/magazine/2024/02/05/can-the-internet-be-governed?> (Accessed: 15.08.2025.).
- Kinne, B.J. (2014): "Dependent diplomacy: signaling, strategy, and prestige in the diplomatic network", *International Studies Quarterly*, 58:2, 247–259.
- Lewis, D. (2014): *Digital Diplomacy*, <http://www.gatewayhouse.in/digital-diplomacy-2/>.
- Manor, I. & C. Segev (2015): "America's Selfie: How the US Portrays Itself on Its Social Media Accounts", in: Bjola, C. & Holmes, M. (eds), *Digital Diplomacy: Theory and Practice*, New York, Routledge.
- Melissen, J. (2013): "Public Diplomacy", in: *The Oxford Handbook of Modern Diplomacy*, 436–452, Oxford, Oxford University Press.
- Osce (2004): *Session 2: Online propaganda and the commission of hate crime*, Michael Whine, <https://www.osce.org/cio/33843>.
- Pamment, J. (2012): *New public diplomacy in the 21st century: A comparative study of policy and practice*, Oxon, Routledge.
- Pashentsev, E. N., & Sebekin, S. (2023): "Metaverses, artificial intelligence and challenges to psychological security" *Politika nacionalne bezbednosti*, (2), 33–37. DOI: 10.5937/pnb25-46760
- Radanliev, P. (2024): "Cyber diplomacy: defining the opportunities for cyber-security and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing", *Journal of Cyber Security Technology*, 9(1), 28–78. DOI: 10.1080/23742917.2024.2312671
- Robinson, R. (2024): *Cyber Diplomacy: A New Frontier in International Relations and Professional Practice*, <https://www.jdsupra.com/legalnews/cyber-diplomacy-a-new-frontier-in-6850511/>.
- Solum, B. (2009): „Models of Internet Governance“ in: Bygrave, L. A., & Bing, J. (Eds.), *Internet Governance: Infrastructure and Institutions* (pp. 48-91), Oxford University Press.
- Thompson, K. (2016): *Changing the Education Paradigm.... But How?*, <https://fishbowlteaching.com/2016/01/changing-education-paradigm-but-how/>.
- Tokat, Y. (2024): *Cyber Diplomacy: Rethinking Statecraft in the Digital Era*, <https://modernndiplomacy.eu/2024/10/19/cyber-diplomacy-rethinking-statecraft-in-the-digital-era>.
- Vasiloiu, I.-C. (2023): „Cyber Diplomacy: A New Frontier for Global Cooperation in the Digital Age“, *Informatica Economica*, Academy of Economic Studies - Bucharest, Romania, vol. 27(1), 41-50.

SAJBER PRETNJE I DIGITALNA DIPLOMATIJA: KOORDINACIJA DRŽAVNIH ODGOVORA U FRAGMENTIRANIM PRAVNIM OKRUŽENJIMA

Sažetak: Digitalni mediji su se pojavili kao ključni igrači u olakšavanju novih oblika interakcije, fundamentalno menjajući način na koji razmišljamo o diplomatiji i nacionalnoj bezbednosti. Rad istražuje digitalnu diplomatiju, modernu strategiju koja omogućava direktnu komunikaciju između državnih aktera, civilnog društva i diplomata putem onlajn kanala. Kršenje podataka, onlajn radikalizacija i izazovi uspostavljanja obaveza i pravne odgovornosti u prekograničnim sajber napadima samo su neka od ozbiljnih pitanja koja donosi globalna priroda sajber prostora. Problem je dodatno složen zbog nepovezanih pravnih sistema koji se često bore da se efikasno nose sa prekograničnim pretnjama. Rad istražuje kako nacionalni zakoni posustaju kada se sajber napadi dogode van granica jedne nacije i skreće pažnju na ozbiljne nedostatke u međunarodnom pravu. Ispituje niz strategija regulacije u kontekstu međunarodnih normi, modele koje vode države, samoregulatorne i kooperativne modele. To uključuje sektorske taktike Sjedinjenih Država, čvrst stav Kine o digitalnom suverenitetu i naglasak EU na digitalnom upravljanju zasnovanom na pravima. Pored toga, globalni napor poput Budimpeštanske konvencije i Talinskog priručnika smatraju se važnim resursima za negovanje međunarodne saradnje. Rastući značaj digitalne diplomatije je posebno primetan, posebno dok se suočavamo sa novim tehnološkim preprekama. Jasno je da nam je potrebno jače diplomatsko obrazovanje, bolja koordinacija među zemljama i pravno utemeljeni mehanizmi saradnje kako bismo se efikasno suprotstavili sajber pretnjama u našem međusobno povezanom svetu.

Ključne reči: Digitalna diplomatija, Digitalni mediji, Pravna regulativa, Međunarodna saradnja