KRAKOWSKIE STUDIA MIĘDZYNARODOWE
KRAKOW INTERNATIONAL STUDIES
XXI: 2024 e-ISSN 2451-0610 ISSN 1733-2680

https://doi.org/10.48269/2451-0610-ksm-2024-006

**Nezir Akyeşilmen**

PhD, Selçuk University
https://orcid.org/0000-0001-8184-5280
nezmen@yahoo.com

# Digital transformation in international relations: new challenges, old strategies?

## Introduction

Discussions on digitalization have recently gained prominence across various disciplines, particularly in international relations, resulting in a substantial body of literature due to its multifaceted impacts. Digitalization fundamentally pertains to the application of various ways and avenues across multiple domains, including communication, banking, security, and the environment. The advancement of cyber technology has led to the emergence of new concepts and policies such as cybersecurity, cyber diplomacy, new frameworks, applications, policies, and strategies within international relations.

The foundation of digital transformation is in the accessibility and efficiency of digital technologies, which are often cost-effective and serve as a significant catalyst for change across several domains. The internet, as a worldwide network, has facilitated the emergence of global interconnectedness and integration through its various applications. The swift advancement of technology and the reciprocal influence of the resulting transformation have significantly altered the discipline of international relations.

Governments have for a long period of time ignored cyber technology. They regarded cyber technology as a non-strategic, low-politics issue in international relations, akin to entertainment, economy, environment, and human rights. Consequently, due to recent advancements in this domain and their transformative impact on international relations, governmental approaches have changed. The DDoS attacks on Estonia in 2007, the hybrid warfare in Georgia in 2008, the Stuxnet attack on Iranian nuclear facilities in 2010, and the Snowden case in 2013 led nations to recognize that cyberspace is not a domain of low politics; rather, high politics, i.e. it is a critical arena for security, military, and strategic considerations. Consequently, nations have been implementing new strategies to enhance security measures and applications in this domain[1].

In various domains, including security, economy, finance, international trade, technology transfer, environmental protection, and human rights, a consensus has developed that this technology enhances the power dynamics of nations. Consequently, nations have commenced the formulation of cyber security strategies, measures, regulations, and applications on a worldwide basis, particularly after Stuxnet in 2010. Cybersecurity has now emerged as a critical element of both national and international security[2].

Digital technology has altered the nature of inter-state relations and empowered non-state actors that become more influential and transformative in international politics. This environment reveals the interplay between national sovereignty disputes in international relations and the influence of big-tech companies, which are significant actors in digital domain.

This study seeks to comprehend the significant impacts of these transformative processes in international relations. Extensive research elucidating this novel, rapid, and dynamic technology, which significantly impacts international relations, remains relatively scarce. This study seeks to elucidate the existing literature gap using a literature review, comparative analyses, illustrative examples, the transformative approach of constructivist theory, and various events and cases.

## Methodology

This work is methodologically organized around two principal axes: the first pertains to the constructivist theory in international relations, which addresses changes in global affairs. The subsequent component is the literature review. In

1 N. Akyeşilmen, *Siber Politika ve Siber Güvenlik*, Orion Kitapevi, Ankara 2018.

2 *Ibidem*.

addition to them, comparisons, statistics, examples, and historical events will be utilized as needed.

## Alteration in constructivist international relations theory

The constructivist theory in international relations posits that the interests and behaviors of actors, including governments, international organizations, individuals, and other non-state entities, are dynamic rather than static. These are typically built socially and evolve around norms, beliefs, and shared ideas. As norms, principles, and regulations evolve, the behaviors, policies, strategies, and interests of these actors likewise transform. Normative shifts in international relations may arise following significant transformations or through social learning processes. The historical example of the banning of slavery in the late 19th century illustrates a significant transformation in the attitudes and actions of nations and other entities about slavery in international relations. Subsequent to the World War II, human rights emerged as a standard in international relations, and by the conclusion of the Cold War, they evolved into both a foundation of legitimacy and a significant norm governing conduct and interactions in international relations. In the recent years, particularly in international relations, significant measures have been implemented, and behaviors have evolved due to environmental protection, climate change, global warming, and heightened awareness[3].

In the 21st century, as the internet has proliferated, we observe that existing international norms have progressively evolved due to digitalization and cyber technology, significantly influencing the conduct of both state and non-state actors in international relations. Within this context, particularly the cybersecurity principles established by the United Nations and other international entities, decisions and measures pertaining to the combat against cyber-crimes have been formulated. There are ongoing norm development activities, albeit inadequate, in cyber security as well as in human rights, digital diplomacy, and cyber conflicts[4].

Over the past 30 years, we have observed numerous advancements in international relations due to digitalization. This procedure has constituted a significant social learning experience for all participants. We are currently observing the steady establishment of new norms, rules, and principles of international

[3] M. Zehfuss, *Constructivism in International Relations*, Cambridge University Press, Cambridge 2002.

[4] *Ibidem*.

law in this domain, facilitated by both innovations and the learning process. The 2024 United Nations Convention on Combating Cyber Crimes, international cyberspace agreements established by the Council of Europe, and various regional organizations, along with the principles and ethical codes in the digital domain formulated by the Tallinn Guide and numerous civil society organizations, serve as significant examples of these initiatives. Consequently, international relations actors, ranging from states to individuals, are compelled to formulate new behaviors, methods, and policies.

## Literature Review

The concept of digital transformation encompasses a dynamic and ongoing process that fundamentally alters the manner in which individuals engage with one another and wider community and its institutions. The absence of a universally acknowledged definition for this concept is a fact. Within the realm of literature, it is evident that there exists a multitude of definitions that vary across different disciplines and among various authors. Drawing upon many sources in the scholarly literature, the present study aims to formulate a working definition for the purpose of this research endeavor. Gregory Vial focuses on the impact of the processes on the entities and defines it

> as a process where digital technologies create disruptions triggering strategic responses from organizations that seek to alter their value creation paths while managing the structural changes and organizational barriers that affect the positive and negative outcomes of this process[5].

On the other hand Kirsten Liere-Netheler and others identify digital transformation as a more comprehensive process,

> a metamorphosis that is based on the intensive combination of present and future technologies that will change the paradigm of how value-generating processes in and between enterprises as well as with customers take place. DT will affect business models and corporate strategies[6].

Strange and others put forward in their definition the usage of variety of technologies and define it as

[5] G. Vial, *Understanding digital transformation: A review and a research agenda*, "Journal of Strategic Information Systems" 2019, vol. 28, issue 2, pp. 118–144.

[6] K. Liere-Netheler, K. Vogelsang, S. Packmohr, U. Hoppe, *Towards a framework for digital transformation success in manufacturing*, Twenty-Sixth European Conference on Information Systems, 2018, www.diva-portal.org/smash/get/diva2:1420340/FULLTEXT01.pdf [accessed: 9.08.2023].

> a process arising from the adoption of a variety of modern technologies for data collection, storage and analytics, such as digital platforms, the Internet of Things (IoT), artificial intelligence (AI), robotic automation, cloud computing, big data analytics, and additive manufacturing (also known as 3D printing)[7].

Based on these and other definitions, digital transformation can be defined as a process of using digital technologies to improve our ways of producing and consuming, our communication and interaction, and our understanding of our social, economic, cultural, strategic, and natural environment. This is done in a way that is enriched by digital technologies, with the use of new concepts, tools, and frameworks.

The potential consequences of digital transformation on international relations encompass several key aspects. Cybersecurity is at the top of the agenda. Then the concepts of cyber power and cyber deterrence are among the primary subjects of discussion. Alongside the continuous development of new cyber weapons and the established traditional deterrence, the question of whether cyber power engenders cyber deterrence remains a significant topic of scholarly discourse. Another significant concern brought about by digitalization in international relations is the challenge of global cyber governance. The question of who will govern the digital domain, now has emerged as a critical issue. The primary concern is the governance of the multi-centric cyber domain. The cyber domain is evolving into a phenomena that exceeds state control and complicates administration due to its multi-actor and multi-stakeholder nature. The artificial intelligence and big data are among two elements that going to transform the discipline. Furthermore, two additional significant challenges arising from digitalization are open diplomacy and human rights in the digital realm. Cyber international relations facilitate the growth of concepts such as digital diplomacy and the use of novel instruments and procedures in diplomatic practice; nevertheless, they also engender concerns over a potential diminishment in the efficacy and reliability of diplomacy. Digitalization has profoundly influenced citizen-state relations across all domains[8].

The existing literature has extensively examined several significant themes, including the effects of digital technologies on state sovereignty, the involvement of digital technologies in conflict and cooperation, the complexities surrounding cyber security and data privacy in the digital era. Digitalization has influenced international relations across various aspects. The anarchic nature of

[7] R. Strang, L. Chen, M.T.L. Fleury, *Digital Transformation and International Strategies*, "Journal of International Management" 2022, vol. 28, issue 4, pp. 1–26.

[8] *Digital trade*, OECD, 2023, www.oecd.org/en/topics/digital-trade.html [accessed: 8.08.2023]; N. Akyeşilmen, *Siber Politika…*, *op. cit.*

cyberspace has exacerbated the level of disorder in international relations, resulting in what Nazli Choucri describes as a hyper-anarchy, akin to a real Hobbesian anarchy. The primary reason for this is that institutions such as international law, international organizations, diplomacy, and big powers, which establish a kind of order in international interactions, are either significantly weakened or entirely absent. Digitalization impacts the actors or agents in international interactions. Although the state occupies a central position in traditional international relations, its influence has diminished somewhat in cyber international relations, suggesting that corporations have emerged as more influential actors in this domain. Although international relations have evolved over territorial boundaries, it is impractical to discuss borders in cyberspace. In cyberspace, both boundaries and distances can be discussed, as distances have become mostly irrelevant. As borders and distances have diminished in significance within international relations, state sovereignty has been considerably undermined. Due to the absence of borders over which nations can assert sovereignty, and the fact that attacks can transpire globally, identifying the perpetrator is very challenging. Furthermore, even when the assailant is located, administering legal punishment has become a complex issue. Cyber conflicts represent a significant novelty introduced by cyberspace and digitalization in international relations. Indeed, while cyber conflicts represent an extension of kinetic conflicts, they have emerged as a novel phenomenon in international relations due to the unique features they introduce to warfare. The fundamental characteristic of cyber wars is their heightened digital nature. Their abundance renders international relations more contentious, however diminishes the degree of violence. The current destructiveness of cyber weapons remains quite minimal[9].

[9] E. Hedling, N. Bremberg, *Practice Approaches to the Digital Transformations of Diplomacy: Toward a New Research Agenda*, "International Studies Review" 2021, vol. 23, issue 4, pp. 1595–1618; A.A. Adonis, *Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy*, "Global: Jurnal Politik Internasional" 2019, vol. 21, no. 2, pp. 262–282; H. Gu, *Data, Big Tech, and the New Concept of Sovereignty*, "Journal of Chinese Political Science" 2024, vol. 29, pp. 591–612; N. Akyeşilmen, *Cybersecurity and Human Rights: Need for a Paradigm Shift?*, "Cyberpolitik Journal" 2016, vol. 1, no. 1, pp. 32–55; *idem*, *Siber Politika*..., *op. cit.*; *Rise Of Artificial Intelligence in Military Weapons Systems: The Need For Concepts and Regulations*, Fraunhofer Group For Defense and Security, 2023, www.vvs.fraunhofer.de/content/dam/iosb/vvs/documents/Positionspapiere/FraunhoferVVS_%20AI-In-Weaponsystems_2 020.pdf [accessed: 19.08.2023]; L. Almagro, L. Kaspar, *National Cybersecurity Strategies: Lessons Learned and Reflections from Americas and Other Regions*, Organization of American States, Global Partners Digital, 2022, www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflec-

The literature concerning the digital realm and international relations is evolving swiftly; yet, a significant deficiency exists in this body of work, particularly with the digitization of international relations. This essay intends to address this deficiency.

## International security

In international relations, security is significantly impacted by digitization. Currently, cyber security has emerged as the key component of both national and international security. The proliferation of the Internet of Things (IoTs) has intensified digitalization, hence complicating security measures. With the IoTs, an increasing number of instruments are connected to the internet, and it is anticipated that all connected devices are hackable, resulting in a growing interconnectedness. Consequently, all internet-connected devices represent a security gap. This exacerbates security challenges[10]. The growing dependence on digital technologies has rendered nations increasingly susceptible to cyber threats. These attacks possess the capability to illicitly acquire confidential information, impair critical infrastructure, or potentially inflict physical harm.

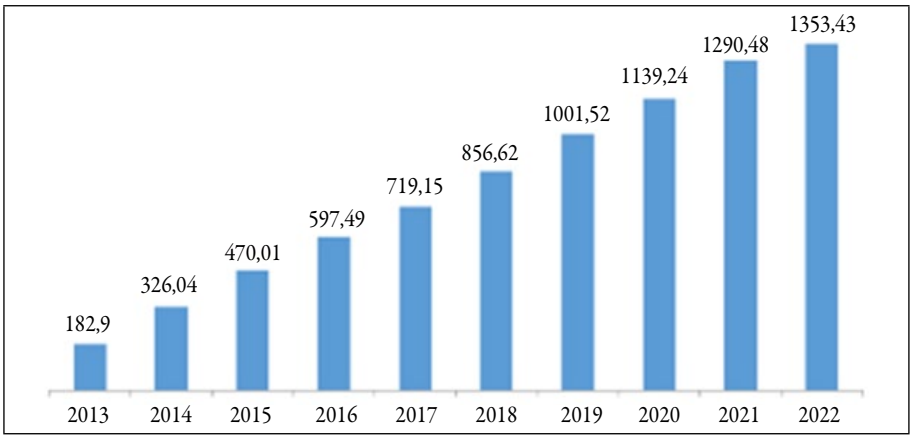
The incidence of cyberattacks has markedly increased with the progression of digitalization. Figure 1 indicates that the daily attack count exceeded 2.5 million. Avast reported experiencing millions of attacks daily. The notable discrepancies can be ascribed to differences in measurement techniques, data sources, geographical coverage, and organizational policies and criteria. The domain of cybersecurity and cyberattacks will evolve concurrently with the swift evolution of technology. As a result, the field of cybersecurity will continually evolve and become increasingly intricate. To maintain ongoing success, governments and the international community must be prepared to adjust to impending developments[11].

tions-ENG.pdf [accessed: 19.08.2023]; E. Haber, L. Topor, *Sovereignty, Cyberspace, and the Emergence of Internet Bubbles*, "Journal of Advanced Military Studies" 2023, vol. 14, no. 1, pp. 144–165.

[10] S. Ohrimenco, C. Valeriu, *Shadow Digital Technologies Threats to National Security*, Conference: Economics, Management, Finance and Banking, Svishtov 2022, www.researchgate.net/publication/363925652_SHADOW_DIGITAL_TECHNOLOGIES_THREATS_TO_NATIONAL_SECURITY [accessed: 17.09.2023].

[11] H.S. Al-Musawi, A.S. Mohammed, *Hybrid Malware Detection and Classification in Real- Time By Deep Learning Techniques 1*, "Proceedings of SAARD International, Putrajaya, Malaysia" 2022, www.researchgate.net/publication/365196411_HYBRID_MALWARE_DETECTION_AND_CLASSIFICATION_IN_REAL_TIME_BY_DEEP_LEARNING_TECHNIQUES_1 [accessed: 8.12.2024]; N. Akyeşilmen,

Figure 1. Malware statistics in millions [2013–2022]




Source: H.S. Al-Musawi, A.S. Mohammed, *Hybrid Malware Detection...*, *op. cit.*, p. 43.

Digitalization can lead to emergence and escalation of cyberwarfare. Cyberwarfare refers to the utilization of digital technology for mainly political reasons of launching attacks or causing disruptions to computer networks and systems[12]. Cyberwarfare with its hybrid and proxy forms has changed landscape of modern warfare. Cyberwarfare occurs when nation-states and non-state actors break into computers or networks to introduce, corrupt, or falsify data, destroy a device, or disrupt computer control systems and launch actions that assist tactical and operational military actions and autonomous strategic impacts. Not only states but also arguably non-state actors including spies, criminals, and hackers can wage cyber war[13]. The utilization of cyber capabilities by both state and non-state actors poses an escalating menace to both national and global security, as it enables the theft of sensitive data, the disruption of critical infrastructure, and the initiation of propaganda campaigns.

One of the consequences of warfare is the utilization of proxy wars, usually facilitated through corporate entities. The utilization of cyberspace as a battleground seems to encompass all the characteristics that have rendered proxy conflicts a preferred choice for actors aiming to achieve their objectives with

*Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice*, "Insight Turkey" 2022, vol. 24, no. 3, pp. 109–134.

12 N. Akyeşilmen, *Siber Politika...*, *op. cit.*

13 A.F. Krepinevich, *Cyber Warfare: A 'Nuclear Option'?*, Center for Strategic And Budgetary Assessments, 2012, https://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf [accessed: 17.08.2023].

minimal risk exposure[14]. The growing dependence on digital technologies is facilitating the utilization of proxies in the realm of cyberspace by nations. The utilization of proxies in the realm of internet is an escalating matter of apprehension for global security. This phenomenon can potentially impede the process of detecting and mitigating intrusions which might also led to de-escalation of conflict and indirectly contribute in international peace. That is why, international powers are currently involved in cyber proxy warfare as a result of the comparatively minimal risk of escalation, numerous obstacles in enforcement, and the lack of clarity surrounding international law in this domain[15]. The possibility of cyber proxy warfare or unwanted foreign influence in general may prompt certain world powers to consider the option of closing or imposing restrictions on their virtual borders.

The advent of digital transformation has concurrently given rise to new challenges pertaining to global security. The advent of digitization has rendered the application of artificial intelligence in various domains, particularly international relations, a contemporary concern. The utilization of artificial intelligence as a surveillance instrument and with the emergence of robotic warrior, complicates the situation further. Simultaneously, it complicates big data and international relations in the domains where big data is utilized[16]. The influence of digital revolution on global security is multifaceted and dynamic. This shift is accompanied by both potential threats and opportunities.

## The rise of digital diplomacy

Digital revolution has significantly influenced the realm of digital diplomacy, manifesting in several notable ways. Digital technologies have the potential to foster interpersonal and intercultural connections, facilitate comprehension, and tackle worldwide issues. The potential outcomes of this development may

[14] M.R. Torres Soriano, *Proxy Wars in Cyberspace*, "Journal of the Spanish Institute for Strategic Studies" 2017, no. 9, pp. 211–230.

[15] E. Haber, L. Topor, *Sovereignty*..., *op. cit.*

[16] D. Cottier, *Emergence of lethal autonomous weapons systems (LAWS) and their necessary apprehension through European human rights law*, report by Council of Europe Committee on Legal Affairs and Human Rights, 2022, https://assembly.coe.int/LifeRay/JUR/Pdf/TextesProvisoires/2022/20221116-LawsApprehension-EN.pdf [accessed: 15.08.2023]; *Rise Of Artificial Intelligence*..., *op. cit.*; *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [accessed: 19.08.2023]; L. Almagro, L. Kaspar, *National Cybersecurity Strategies*..., *op. cit.*

encompass new prospects in the field of diplomacy[17]. The enhanced connectivity of the global community has facilitated more efficient communication between governments and their populations, as well as among different countries and other stakeholders of international relations. The increasing utilization of digital technology for diplomatic objectives, including but not limited to social media, video conferencing, and online messaging platforms, has become evident.

Digitalization of diplomacy has profoundly affected all four dimensions of diplomacy. These dimensions can be specified as the institutional structure of diplomacy, diplomacy executives, those affected by diplomacy and the method of execution of diplomacy. The digitalization of diplomacy results in the modification and transformation of diplomatic norms and practices. Even though US President Donald Trump's Twitter diplomacy[18] has been criticized for not being suitable for diplomatic practices, it is also a sign that the institutional structure of diplomacy will change with the advent of the digital age. In addition, digital diplomacy presents diplomatic leaders with both challenges and opportunities. Diplomacy executives have the ability to reach large audiences and communicate with them, which is advantageous. However, the absence of error feedback makes it difficult for them to correct errors. In addition, digitalization blurs the distinction between those who are affected by diplomacy and those who conduct diplomacy. Finally, significant changes are occurring in the execution of diplomacy. Currently, as a result of the pandemic, there are more online conversations and digital technologies are being utilized more frequently in diplomacy[19].

Technological progress enables the emergence of new diplomatic actors. Established actors must also modify their techniques and public image. Digital diplomacy's disruptive effect on traditional diplomatic practices can be attributed to its experimental nature[20]. Digital technology have also facilitated enhanced openness in governmental operations, enabling more efficient dissemination of information to the general public[21]. The aforementioned development has resulted in enhanced transparency within the diplomatic process, hence facilitating the ability of individuals to effectively scrutinize and demand

17 E. Hedling, N. Bremberg, *Practice Approaches…*, *op. cit.*; B. Hocking, J. Melissen, *Diplomacy in the Digital Age*, Clingendael – the Netherlands Institute of International Relations, 2015, www.clingendael.org/sites/default/files/pdfs/Digital_Diplomacy_in_the_Digital%20Age_Clingendael_July2015.pdf [accessed: 10.09.2023].

18 @realDonaldTrump has 95,7 million followers [accessed: 8.12.2024].

19 H. Aktaş, *Digital Diplomacy and its Implications in The 21st Century*, Antalya Diplomatic Forum, 2021, https://antalyadf.org/wp-content/uploads/2021/01/Digital-Diplomacy-and-Its-Implications-In-The-21st-Century.pdf [accessed: 10.08.2023].

20 E. Hedling, N. Bremberg, *Practice Approaches…*, *op. cit.*

21 H. Aktaş, *Digital Diplomacy…*, *op. cit.*

accountability from their own governments. Digital technologies have ushered in novel instruments for governments to foster engagement with citizens and other stakeholders. This phenomenon has facilitated the establishment of diplomatic ties and the advancement of national agendas by governments.

The process of digitization is significantly altering the modes of communication and interaction employed by diplomats. Historically, diplomats have heavily relied on conventional means of communication such as in-person meetings, telephone conversations, and written correspondence to engage in inter-diplomatic discourse. In contemporary times, social networking, video conferencing, and various digital tools are commonly employed. As Elsa Hedling[22] put forward "Digital diplomacy today is much more than world leaders' use of Twitter. Itis a fundamental dimension of contemporary international politics"[23].

Nevertheless, the process of digitization is concurrently giving rise to new obstacles in the realm of diplomacy. One significant obstacle is in the proliferation of inaccurate information. Historically, disseminating misinformation on a significant scale posed a formidable challenge for individuals. In contemporary times, the facilitation of such tasks has been significantly enhanced owing to the advent of social media platforms and several other digital resources[24]. Another notable challenge pertains to the insufficient proficiency or capability in effectively utilizing digital diplomatic instruments among foreign policy decision-makers. However, a further challenge arises from the linguistic disparities between digital platforms, particularly social media platforms, and conventional diplomatic discourse. Lastly, the process of digitization entails increased velocity, which often results in errors, a factor that is not conducive to the realm of diplomacy where errors are generally not tolerated. These phenomena might pose challenges to diplomats in terms of successful intercommunication and the establishment of confidence with foreign nations.

## The changing nature of power and influence

The implications of digital transformation on the changing dynamics of power and influence in the field of international relations can be summarized as the emergence and growth of non-state actors, the erosion of state sovereignty, development of new sources of influence and the need for cooperation among all stakeholders in cyber domain.

---

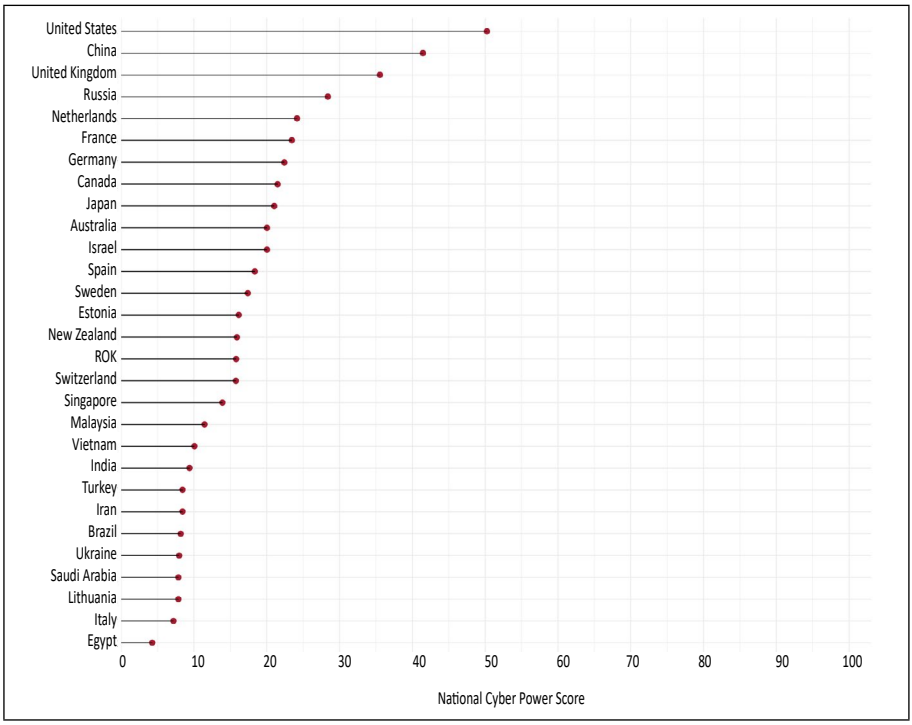
22 *Ibidem.*

23 *Ibidem.*

24 N. Akyeşilmen, *Cybersecurity*..., *op. cit.*; *idem*, *Siber Politika*..., *op. cit.*

Firstly, cyber technology introduces a novel dimension to power, termed cyber power, which is indeed a highly powerful component. Terms like cyber power and cyber deterrent are now prevalent in international affairs. Regardless of the various definitions proposed, According to Julia Voo Nezir Akyeşilmen, cyber power is defined as the capabilities to accomplish desired objectives. Cyber capabilities pertain to the development, management, and transmission of electronic and computer-based information systems, networks, software, and human expertise. Consequently, nations allocate resources across several domains, including military cyber capabilities, cyber defence, surveillance, human capacity development, institutional fortification, and domestic policy enhancement[25]. The National Cyber Power Index (NCPI), developed by the Cambridge Belfer Center, evaluates the cyber capabilities of 30 nations. NCPI evaluates nations' intentions and capacities across multiple domains, including surveillance, defence, control, intelligence, trade, offense, and norms.

Figure 2. Most comprehensive cyber powers




Source: J. Voo, I. Hemani, S. Jones, W. DeSombre, *National Cyber Power Index 2020: Methodology and Analytical Considerations*, Belfer Centre for Science and International Affairs, p. 11, www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf [accessed: 8.12.2024].

[25] *Idem*, *Türkiye in the Global Cybersecurity Arena...*, *op. cit.*

The nations exhibiting the highest degree of intent and capability across all seven objectives, sorted by comprehensiveness as illustrated in figure 2 are as follows: United States (50), China (47), United Kingdom (36), Russia (29), Netherlands (25), France (24), Germany (23), Canada (22), Japan (21), Australia (20). Turkey ranks 22nd among 30 countries, achieving a score of 9. Turkey's ranks in each subsection are as follows: surveillance (19th), defence (21st), information control (28th), intelligence (27th), commerce (29th), offense (19th), and norms (21st)[26].

Cyber non-state actors (CNSAs) play a crucial role in the contemporary globalized landscape, as their activities has the potential to exert substantial influence on international affairs, politics, and the economy, comparable to that of nation-states. Non-state actors encompass a wide range of entities, such as multinational corporations, hacktivist collectives, non-governmental organizations (NGOs), cybercrime syndicates, private military organizations, media outlets, terrorist groups, labor unions, organized ethnic groups, lobby groups, criminal organizations, private businesses, and various other entities[27]. This phenomenon has posed challenges for states in their efforts to exert control and influence over these individuals. The frequency and complexity of cyber-attacks are on the rise.

The notion of sovereignty is a crucial political ideal that has persisted throughout human history, spanning several centuries. Nevertheless, the advent of the industrial revolution and the subsequent trend of globalization has engendered its widespread application across all geographical regions. Subsequently, it has emerged as the fundamental principle of the contemporary international order, having endured and surpassed all competing ideologies. The advent of the digital realm has presented new challenges to the notion of sovereignty. The erosion of sovereignty can manifest in various ways, including diminished state control over borders and citizens particularly due to new technologies such as blockchain, AI and cloud technology, weakened enforcement of national laws to the point of invalidation, increased vulnerability to cyberattacks, enhanced empowerment of non-state actors, and the potential disruption of state income through the utilization of cryptocurrency. The reason for this phenomenon is because states are no longer able to exert control over the dissemination of

[26] N. Akyeşilmen, *Türkiye in the Global Cybersecurity Arena*..., *op. cit.*; J. Voo, I. Hemani, S. Jones, W. DeSombre, *National Cyber Power Index 2020*..., *op. cit.*

[27] P. Paganini, *Non-State Actors in Cyberspace: An Attempt to a Taxonomic Classification, Role, Impact And Relations with a State's Socio-Economic Structure*, Center for Cyber Security and International Relations Studies, 2022, www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf [accessed: 2.09.2023].

information within their respective territories[28]. The Arab Spring, a significant political movement, was predominantly enabled by the utilization of social media platforms. This technological medium provided activists with a means to effectively coordinate and exchange information, while mitigating concerns of potential retaliation from governing authorities[29].

The advent of digital transformation has given rise to new obstacles that necessitate global cooperation. One such instance is to the imperative of addressing cyberattacks and disinformation, as well as the necessity of implementing legal and administrative regulatory measures for emerging technology[30]. The effective resolution of these difficulties necessitates international collaboration, international cyber law, ethical and responsible use of technology and a holistic approach to security that encompasses individual, societal, national, international and global security as interconnected and interdependent.

## The impact on democracy and human rights

Digitalization exerts varying impacts on democratization and human rights. Significant beneficial impacts on democracy may be observed; for instance, direct democracy could reemerge as a pertinent topic. Should a secure internet be established and the societal perception of eradicated frauds be cultivated, the implementation of direct democracy becomes feasible. Moreover, promoting engagement in certain processes enhances the applicability of participatory and deliberative democracy, hence increasing the reliability of the democratic system through transparency and access to information.

Digitalization has profoundly influenced citizen-state relations across all domains. In this context, with emerging conversations on digital citizenship, we observe some impacts on the framework for safeguarding and advancing human rights. Digital citizenship introduces new obligations and rights for individuals, necessitating the acquisition of additional skills. Digital citizenship entails the ethical, responsible, and secure utilization of digital platforms, necessitating the safeguarding of one's own rights as well as the rights of others on these

[28] A.A. Adonis, *Critical Engagement*..., *op. cit.*; H. Gu, *Data, Big Tech*..., *op. cit.*

[29] K.Z. Meral, Y. Meral, *The Role of Social Media in Arab Spring*, "e-Journal of New Media / Yeni Medya Elektronik Dergi" 2021, vol. 5, issue 1, pp. 26–34.

[30] *International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity*, Information Security Policy Council, 2013, www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf [accessed: 19.08.2023].

platforms[31]. This matter inherently raises concerns regarding human rights in the digital realm. Digitalization exerts three fundamental impacts on human rights. These aim to initiate new discussions in the literature of human rights, to change the nature of some specific rights, such as privacy, and ultimately, to have positive/negative impacts on each right individually within the broader context of human rights as a whole[32].

## The implication for the global trade and commerce

The global economy is being significantly influenced by digital technologies.

> Digitalisation increases the scale, scope and speed of trade. It allows firms to bring new products and services to a larger number of digitally-connected customers across the globe. It also enables firms, notably smaller ones, to use new and innovative digital tools to overcome barriers to growth, helping facilitate payments, enabling cooperation, avoiding investment in fixed assets through the use of cloud-based services, and using alternative funding mechanisms such as crowdfunding[33].

The rise of digital commerce is another benefit of digitization. The expansion of online shopping, for instance, has allowed companies to reach consumers in every corner of the globe that enhance international trade and commerce. Not only companies but also countries strive to increase their share in global digital commerce. In order to attain more equity in the context of digital trade, it is imperative for governments and various stakeholders to collaborate in formulating and executing relevant legislative measures, alongside offering international development assistance[34].

However, the digital revolution is also posing new challenges for business and trade. The proliferation of cybercrime is a challenge. Theft, fraud, and

---

31 *Digital citizenship education*, Council of Europe, 2023, www.coe.int/en/web/digital-citizenship-education/target-groups [accessed: 5.09.2023]; N. Akyeşilmen, *Türkiye in the Global Cybersecurity Arena…*, *op. cit*.

32 K.S. Chauhan, *Human Rights in Cyberspace*, 2023, www.academia.edu/12230260/Human_rights_in_cyberspace [accessed: 5.09.2023]; M. Dvojmoč, M.T. Verboten, *Cyber (In)security of Personal Data and Information in Times of Digitization*, "Medicine Law & Society" 2022, vol. 15, no. 2, pp. 287–304; G. Lucas, *Privacy, Anonymity, and Cyber Security*, "Amsterdam Law Review" 2013, vol. 5, no. 2, pp. 107–114.

33 *Digital trade*, OECD, *op. cit*.

34 *Digital trade: Opportunities and actions for developing countries*, United Nations Conference On Trade And Development, "Policy Brief" 2022, no. 92, https://unctad.org/system/files/official-document/presspb2021d10_en.pdf [accessed: 7.09.2023].

vandalism are all examples of cybercrime since they include the use of digital means[35].

## The impact on the environment

Digital transformation can significantly enhance efforts to protect and improve the environment. One approach is to implement more effective methods utilizing big data to address environmental issues[36]. Another significant aspect is that certain processes can be subjected to automatic scrutiny, hence facilitating environmental protection through reduced energy consumption.

Digital change can potentially exert adverse effects on the environment. For instance, digital technologies have the potential to augment energy consumption as their manufacture and utilization necessitate energy, hence potentially exacerbating climate change. The environmental consequences of digital products are primarily associated with the utilization of resources and energy, encompassing the production of information and communication technology devices, energy usage, and the management of electronic waste. Mining and extraction of natural resources necessary for the production of physical products are the main factors contributing to resource depletion and global warming. In addition, it is worth noting that the emissions of greenhouse gases resulting from the generation of power may exert an impact on biodiversity[37].

## The need for a new theory of international relations

Traditional International Relations theories aim to elucidate political phenomena within physical spaces, encompassing land, sea, air, and outer space. However, a new realm has emerged, commonly referred to as cyberspace. As some unique features such as time, space, anonymity, ubiquity, permeation and

[35] N. Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, "Vanderbilt Journal of Transnational Law" 2019, vol. 52, no. 463, pp. 463–509.

[36] T.C. Truong, *The Impact of Digital Transformation on Environmental Sustainability*, "Advances in Multimedia" 2022, no. 3, pp. 1–12; P. Ghostal, *The Environmental Impact of Digitalisation: What's Your Take on Sustainable Technology?*, FDM, 22.08.2023, www.fdmgroup.com/news-insights/environmental-impact-of-digitalisation [accessed: 7.09.2023]; G. Babinet, *The Environmental Impact and Potential of Digital Technology*, Institut Montaigne, 2021, www.institutmontaigne.org/en/expressions/environmental-impact-and-potential-digital-technology [accessed: 7.09.2023].

[37] *Ibidem*.

hyper-anarchy. Conventional theories lack the necessary tools to analyze and elucidate advancements within this new and distinct domain. In recent years, the literature in the discipline has revolved on the necessity of developing a new conceptual and theoretical framework to effectively comprehend the dynamics of international political processes within the realm of cyberspace[38].

To conclude, it is imperative to acknowledge that the potential consequences of digital transformation are not exclusively adverse. Digital technologies can also serve as a means to advance peace, security, and prosperity. Digital technologies have the potential to enhance communication and collaboration among nations, facilitate the provision of humanitarian aid, and foster educational advancement and socio-economic growth[39].

## Findings and analysis

Through the analyses conducted throughout the article, several vital findings have been addressed. Digital technologies, because to their dynamic nature, will transform more international relations in near future. Comprehending the alterations and shifts induced by digitalization in international relations, and therefore formulating policies and plans to adeptly evaluate the benefits and challenges posed by cyber technology, is exceedingly advantageous.

The impact of digitalization on the theory and practice of international relations requires more analysis from various viewpoints. Primarily, it is clear that conventional international relations theories inadequately account for the processes and innovations transpiring in the digital domain. Consequently, a new theory is required to elucidate the behaviours, political processes, and interactions of actors in cyber international relations[40]. To understand the intricate realm of cyber international relations and formulate effective tactics, it is essential to foster new approaches. Cyber conflicts constitute a novel issue in international relations, necessitating the implementation of new techniques, processes, and measures for effective governance and resolution. The advent of new hybrid wars is an unavoidable fact, and within this framework,

[38] N. Akyeşilmen, *Siber Politika*..., *op. cit.*; N. Choucri, *Cyberpolitics in International Relations*, The MIT Press, Cambridge–London 2012, https://flavioufabc.wordpress.com/wp-content/uploads/2017/02/cyberpolitics-and-international-relations.pdf?fbclid=IwAR3k02bKQQAag2mTr0_vu0VfoKTujMKFSbd8NGFt03Kqyxv9nkGdPCAiOZg [accessed: 11.09.2023].

[39] G.U. Osimen, C. Ronke, *The Impact of Modern Technologies on Peace, Security and Development in Africa*, "Canadian Social Science" 2023, vol. 19, no. 2, pp. 75–82.

[40] A.A. Adonis, *Critical Engagement*..., *op. cit.*

the application of both big data and artificial intelligence will induce substantial transformations.

Artificial intelligence can facilitate a deeper comprehension of social dynamics and political processes, in addition to fostering the formulation of improved policies and strategies. Likewise, technology like blockchain can enhance record accuracy and promote transparency in diplomatic communications. To ensure these changes benefit humanity, particularly scholars and intellectuals must formulate effective solutions. Adopting a proactive and comprehensive approach across all domains is crucial, encompassing security, trade, cooperation, conflict, social life, and environmental protection.

## Discussions

The findings of this article will have significant implications for the theory and practice of international relations, the future framework of the discipline, and the developments awaiting us in the practical application of the global affairs.

Digitalization has significantly affected all domains over the past three decades, including international relations, and continues to exert its influence. Traditional international relations theories were formulated before to the digital age, rendering them inadequate in comprehending this new epoch due to their deficiency of concepts, structures, and methodologies suitable for analyzing the digital domain. Nonetheless, the field of international relations has consistently excelled in formulating or modifying theories to elucidate new situations and transformations[41]. Consequently, it is imperative to provide a novel theoretical framework to elucidate, assess, and appraise the opportunities and challenges presented by the digital realm.

The evolution of innovative diplomatic instruments, techniques, and strategies has emerged as an urgent necessity in the practice of international interactions. Digital diplomacy, utilizing innovative approaches and tools, has the capacity to make substantial contributions in this domain[42]. Nonetheless, it also has certain drawbacks in comparison to conventional diplomacy. These encompass communication problems, dependence on technology, and, most significantly, concerns with diplomatic confidentiality. To sum up, digitalization has significantly influenced high politics, i.e. strategy, military, and

[41] N. Akyeşilmen, *Siber Politika*..., *op. cit.*; N. Choucri, *Cyberpolitics in International Relations*, *op. cit.*

[42] E. Hedling, N. Bremberg, *Practice Approaches*..., *op. cit.*; H. Aktaş, *Digital Diplomacy*..., *op. cit.*

security matters in international relations. To facilitate the discipline's adaptation to this novel process, environment, and domain in both theory and practice, governments, strategists, and intellectuals must devise new tactics, tools, frameworks, and applications[43].

The digital realm presents not just hazards, threats, and security issues but also new opportunities, particularly concerning the interaction between citizens and the state. It generates opportunities in ethics, human rights, the environment, and trade, while concurrently posing certain risks. Inclusive policies are essential for safeguarding and advancing human rights in the digital sphere, humanizing the digital landscape, enhancing environmental protection, and allowing the Global South to reap greater benefits from international free trade. Digitalization certainly, offers novel opportunities to attain these objectives.

Although cyber technology and digitalization are significantly altering international relations, the impact of this transformation on social and political processes, as well as on theoretical frameworks has been gradual and arduous. In this framework, the fact expressed by Eric Schmidt in 2007 remains pertinent today. In many ways the Internet is the world's largest experiment in anarchy. 'The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had'[44].

This insight remains pertinent, as no theoretical framework has been established in international relations or any other field to elucidate the conduct of actors in cyberspace. Thus, an area that has not been theorized is one that stays misconstrued.

## Conclusion

The following are some concluding reflections on the prospective trajectory of digital revolution in domain of international relations. The precise ramifications of digital transformation will be contingent upon the particular circumstances.

It is imperative to establish ethical frameworks or codes of conduct that govern the utilization of digital technologies, so ensuring their appropriate deployment. A transparent and democratic framework for producing, storing,

[43] A.F. Krepinevich, *Cyber Warfare*..., *op. cit.*; D. Cottier, *Emergence of lethal autonomous weapons systems*..., *op. cit.*; *Rise Of Artificial*..., *op. cit.*; E. Haber, L. Topor, *Sovereignty*..., *op. cit.*

[44] E. Schmidt, *American computer executive*, [in:] S. Ratcliffe (ed.), *Oxford Essential Quotations*, 4th ed., Oxford University Press, 2016, www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00017947 [accessed: 8.12.2024].

using, disseminating and governing data is inevitable for the current world politics. And the utilization of digital technology for the purpose of monitoring and addressing possible hazards.

There are several measures that can be implemented to mitigate the hazards associated with the utilization of cyber threats in digital domain. One of the key strategies to address cybersecurity concerns is the enhancement of global cooperation among all stakeholders[45]. The promotion of responsible utilization of digital technologies can be facilitated by cyber actors through the establishment of codes of conduct governing the usage of platforms such as social media[46]. Additionally, efforts should be made to enhance public awareness of the potential threats associated with digitalization processes. Furthermore, it is crucial to implement administrative and legal regulations pertaining to cyber security, including the formulation of national cyber security strategy documents, establishment of cyber incidents response teams, creation of cyber security institutions such as a national coordinator for cyber security, fostering the development of a cyber security culture within society, and promoting education that enhances individual and society capabilities such as digital citizenship education. These measures play a significant role in mitigating cybersecurity threats and challenges.

The consequences and recommendations for future research on digital transformation in the field of international relations are extensive and diverse. Future research should investigate the various modalities through which social media is employed within the context of international relations, and the resultant ramifications for the realm of global governance. In addition, further investigation is necessary to examine the ethical and legal ramifications associated with the utilization of artificial intelligence (AI) within the realm of international relations.

---

[45] *International Strategy on Cybersecurity Cooperation…*, *op. cit.*

[46] B. Hogeveen, *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*, Australian Strategic Policy Institute, 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf [accessed: 12.08.2023]; *Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives*, OECD, 2020, https://mneguidelines.oecd.org/Digitalisation-and-responsible-business-conduct.pdf [accessed: 12.08.2023]; B.S. Buckland, F. Schreier, T.H. Winkler, *Democratic Governance Challenges of Cyber Security*, "DCAF Horizon 2015 Working Paper", no. 1, www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf [accessed: 12.08.2023].

## References


Adonis A.A., *Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy*, "Global: Jurnal Politik Internasional" 2019, vol. 21, no. 2, pp. 262–282.

Aktaş H., *Digital Diplomacy and its Implications in the 21st Century*, Antalya Diplomatic Forum, 2021, https://antalyadf.org/wp-content/uploads/2021/01/Digital-Diplomacy-and-Its-Implications-In-The-21st-Century.pdf [accessed: 10.08.2023].

Akyeşilmen N., *Cybersecurity and Human Rights: Need for a Paradigm Shift?*, "Cyberpolitik Journal" 2016, vol. 1, no. 1, pp. 32–55.

Akyeşilmen N., *Siber Politika ve Siber Güvenlik*, Orion Kitapevi, Ankara 2018.

Akyeşilmen N., *Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice*, "Insight Turkey" 2022, vol. 24, no. 3, pp. 109–134.

Almagro L., Kaspar L., *National Cybersecurity Strategies: Lessons Learned and Reflections from Americas and Other Regions*, Organization of American States, Global Partners Digital, 2022, www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf [accessed: 19.08.2023].

Al-Musawi H.S., Mohammed A.S., *Hybrid Malware Detection and Classification in Real- Time By Deep Learning Techniques 1*, "Proceedings of SAARD International, Putrajaya, Malaysia" 2022, www.researchgate.net/publication/365196411_HYBRID_MALWARE_ DETECTION_AND_CLASSIFICATION_IN_REAL_TIME_BY_DEEP_LEARNING_TECHNIQUES_1 [accessed: 8.12.2024].

Babinet G., *The Environmental Impact and Potential of Digital Technology*, Institut Montaigne, 2021, www.institutmontaigne.org/en/expressions/environmental-impact-and-potential-digital-technology [accessed: 7.09.2023].

Buckland B.S., Schreier F., Winkler T.H., *Democratic Governance Challenges of Cyber Security*, "DCAF Horizon 2015 Working Paper", no. 1, www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf [accessed: 12.08.2023].

Chauhan K.S., *Human Rights in Cyberspace*, 2023, www.academia.edu/12230260/Human_rights_in_cyberspace [accessed: 5.09.2023].

Choucri N., *Cyberpolitics in International Relations*, The MIT Press, Cambridge–London 2012, https://flavioufabc.wordpress.com/wp-content/uploads/2017/02/cyberpolitics-and-international-relations.pdf?fbclid=IwAR3k02bKQQAag2mTr0_vu0VfoKTujMKFSbd8NGFt03Kqyxv9nkGdPCAiOZg [accessed: 11.09.2023].

Cottier D., *Emergence of lethal autonomous weapons systems (LAWS) and their necessary apprehension through European human rights law*, report by Council of Europe Committee on Legal Affairs and Human Rights, 2022, assembly.coe.int/LifeRay/JUR/Pdf/TextesProvisoires/2022/20221116-LawsApprehension-EN.pdf [accessed: 15.08.2023].

*Digital citizenship education*, Council of Europe, 2023, www.coe.int/en/web/digital-citizenship-education/target-groups [accessed: 5.09.2023].

*Digital trade*, OECD, 2023, www.oecd.org/en/topics/digital-trade.html [accessed: 8.08.2023].

*Digital trade: Opportunities and actions for developing countries*, United Nations Conference On Trade And Development, "Policy Brief" 2022, no. 92, unctad.org/system/files/official-document/presspb2021d10_en.pdf [accessed: 7.09.2023].

*Digitalisation and Responsible Business Conduct: Stocktaking of policies and initiatives*, OECD, 2020, https://mneguidelines.oecd.org/Digitalisation-and-responsible-business-conduct.pdf [accessed: 12.08.2023].

Dvojmoč M., Verboten M.T., *Cyber (In)security of Personal Data and Information in Times of Digitization*, "Medicine Law & Society" 2022, vol. 15, no. 2, pp. 287–304.

Ghostal P., *The Environmental Impact of Digitalisation: What's Your Take on Sustainable Technology?*, FDM, 22.08.2023, www.fdmgroup.com/news-insights/environmental-impact-of-digitalisation [accessed: 7.09.2023].

Gu H., *Data, Big Tech, and the New Concept of Sovereignty*, "Journal of Chinese Political Science" 2024, vol. 29, pp. 591–612.

Haber E., Topor L., *Sovereignty, Cyberspace, and the Emergence of Internet Bubbles*, "Journal of Advanced Military Studies" 2023, vol. 14, no. 1, pp. 144–165.

Hedling E., Bremberg N., *Practice Approaches to the Digital Transformations of Diplomacy: Toward a New Research Agenda*, "International Studies Review" 2021, vol. 23, issue 4, pp. 1595–1618.

Hocking B., Melissen J., *Diplomacy in the Digital Age*, Clingendael – the Netherlands Institute of International Relations, 2015, www.clingendael.org/sites/default/files/pdfs/Digital_Diplomacy_in_the_Digital%20Age_Clingendael_July2015.pdf [accessed: 10.09.2023].

Hogeveen B., *The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN*, Australian Strategic Policy Institute, 2022, https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf [accessed: 12.08.2023].

*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [accessed: 19.08.2023].

*International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity*, Information Security Policy Council, 2013, www.nisc.go.jp/eng/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf [accessed: 19.08.2023].

Krepinevich A.F., *Cyber Warfare: A 'Nuclear Option'?*, Center for Strategic And Budgetary Assessments, 2012, https://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf [accessed: 17.08.2023].

Liere-Netheler K., Vogelsang K., Packmohr S., Hoppe U., *Towards a framework for digital transformation success in manufacturing*, Twenty-Sixth European Conference on Information Systems, 2018, www.diva-portal.org/smash/get/diva2:1420340/FULLTEXT01.pdf [accessed: 9.08.2023].

Lucas G., *Privacy, Anonymity, and Cyber Security*, "Amsterdam Law Review" 2013, vol. 5, no. 2, pp. 107–114.

Meral K.Z., Meral Y., *The Role of Social Media in Arab Spring*, "e-Journal of New Media / Yeni Medya Elektronik Dergi" 2021, vol. 5, issue 1, pp. 26–34.

Mishra N., *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, "Vanderbilt Journal of Transnational Law" 2019, vol. 52, no. 463, pp. 463–509.

Ohrimenco S., Valeriu C., *Shadow Digital Technologies Threats to National Security*" Conference: Economics, Management, Finance and Banking, Svishtov, 2022, www.researchgate.net/publication/363925652_SHADOW_DIGITAL_TECHNOLOGIES_THREATS_TO_NATIONAL_SECURITY [accessed: 17.09.2023].

Osimen G.U., Ronke C., *The Impact of Modern Technologies on Peace, Security and Development in Africa*, "Canadian Social Science" 2023, vol. 19, no. 2, pp. 75–82.

Paganini P., *Non-State Actors in Cyberspace: An Attempt to a Taxonomic Classification, Role, Impact And Relations with a State's Socio-Economic Structure*, Center for Cyber Security and International Relations Studies, 2022, www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf [accessed: 2.09.2023].

*Rise Of Artificial Intelligence in Military Weapons Systems: The Need For Concepts and Regulations*, Fraunhofer Group For Defense and Security, 2023, www.vvs.fraunhofer.de/content/dam/iosb/vvs/documents/Positionspapiere/FraunhoferVVS_%20AI-In-Weaponsystems_2020.pdf [accessed: 19.08.2023].

Schmidt E., *American computer executive*, [in:] S. Ratcliffe (ed.), *Oxford Essential Quotations*, 4 ed., Oxford University Press, 2016, www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00017947 [accessed: 8.12.2024].

Strang R., Chen L., Leme M.T.F., *Digital Transformation and International Strategies*, "Journal of International Management" 2022, vol. 28, issue 4, pp. 1–26.

Torres Soriano M.R., *Proxy Wars in Cyberspace*, "Journal of the Spanish Institute for Strategic Studies" 2017, no. 9, pp. 211–230.

Truong T.C., *The Impact of Digital Transformation on Environmental Sustainability*, "Advances in Multimedia" 2022, no. 3, pp. 1–12.

Vial G., *Understanding digital transformation: A review and a research agenda*, "Journal of Strategic Information Systems" 2019, vol. 28, issue 2, pp. 118–144.

Voo J., Hemani I., Jones S., DeSombre W., *National Cyber Power Index 2020: Methodology and Analytical Considerations*, Belfer Centre for Science and International Affairs, 2020, www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf [accessed: 8.12.2024].

Zehfuss M., *Constructivism in International Relations*, Cambridge University Press, Cambridge 2002.

## Abstract

Digitalization has been profoundly affecting every aspect of life for the last three decades including international relations. This study investigates the transformative effects of digitalization on both the discipline of International Relations (IR) and the practice of IR. Digitalization has driven significant transformations across various domains, including from conflict to peace, from diplomacy to security and from human rights to the environment. This study seeks to answer the question of how digitalization has reshaped traditional paradigm of international relations? Adopting a qualitative research methodology, including a comprehensive literature review, also incorporates the Constructivist IR theory, which

emphasizes the changes in actor behaviors occur as norms evolve. The finding reveals a dual impact: While cyber-attacks, especially on critical infrastructures pose threats to national and international security, cyber diplomacy enhances environmental protection and cooperation among global actors. This duality clearly demonstrates how complex and complicated the relationship is between the challenges and opportunities brought about by the digital age in international relations.
**Key words:** international relations, digital transformation, cybersecurity, digital diplomacy and cyber conflicts