RESEARCH ARTICLE

AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

# THE IMPACT OF DIGITAL TECHNOLOGY ON INTERNATIONAL RELATIONS: THE CASE OF THE WAR BETWEEN RUSSIA AND UKRAINE

***Mohamad Albakjaji and Reem Almarzoqi***

Submitted on 25 Jan 2023 / Revised 06 Feb 2023 / Approved **17 Feb 2023**
Published online: **23 Mar 2023** // Last Published: **15 May 2023**

**Summary:** 1. Introduction. – 2. New Technologies as a spatial turn and Paradigms of International Relations. – 3. Technology and a New International Distribution of Power. – 4. Role of New Technologies as a driving force in the social construction of war and peace. – 5. The Aspects of New Technologies Involvement in International Relations: The Russian invasion on Ukrainian territories as an example. – *5.1. The absence of a binding legal framework to regulate the activities of the cyber domain. – 5.2. The Russian-Ukrainian war and the emergence of a new type of sanctions at the international level. – 5.3 Conflict and Technology: The emergence of Digital Currency as a challenge to international relations.* – 6. Legal gaps in legal frameworks when addressing the impact of digital technologies in international relations – 7. Conclusion.

**Keywords:** New Technology, International Relations, War, Russia, Ukraine.

**Mohamad Albakjaji**
PhD in Law, Assistant Professor at the College of law at Prince Sultan University, Saudi Arabia mabkjaji@psu.edu.sa https://orcid.org/0000-0001-5160-0530?lang=en
**Corresponding author**, responsible for writing and research. **Competing interests**: Any competing interests were declared by the author. **Disclaimer**: The author declares that his opinion and views expressed in this manuscript are free of any impact of any organizations.
**Funding**: The authors would like to thank Prince Sultan University for supporting this publication. Special acknowledgement is given to the Governance and Policy Design Research Lab (GPDRL) at Prince Sultan University for their academic support to conduct this research and publish it in a reputable journal.
**Translation**: The content of this article was translated with the participation of third parties under the authors' responsibility.
**Managing editor** – Mg Polina Siedova. **English Editor** – Lucy Baldwin.

**How to cite**: Mohamad Albakjaji and Reem Almarzoqi 'The Impact of Digital Technology on International Relations: The Case of the War between Russia and Ukraine' 2023 2 (19) Access to Justice in Eastern Europe 8–24. https://doi.org/10.33327/AJEE-18-6.2-a000203
**Reem Almarzoqi**
Legal Researcher, Advisor, Legal Advisor at TAWAL Telecommunication Company, Saudi Arabia.
**Co-author**, responsible for writing and research. **Competing interests**: Any competing interests were declared by the author. **Disclaimer**: The author declares that her opinion and views expressed in this manuscript are free of any impact of any organizations, including the TAWAL Telecommunication Company.

## ABSTRACT

***Background:*** *The concept of a strong state is no longer measured by its military and economic strength, but also by the level of its ability to both defend against cyber-attacks and control cyberspace. During the Russian invasion of Ukraine, it became clear that modern technology had an active role on the ground. This research focuses on the role of modern technology in conflicts and as a key factor in relations between states. It has been proven that technology has led to the creation of new concepts in international relations - the concept of technological sanctions, electronic warfare, and so on. This paper will focus deeply on studying the impact of technology on international relations, and its role in war, peace and security. The researcher uses the Russian-Ukrainian war to support these ideas.*

***Methods:*** *In this paper, the researcher used an analytical and structural method to provide an in-depth perspective on the impact of new technology on international relations. Moreover, a case study on the war between Russia and Ukraine were deployed to explain how new technology is heavily involved in international relations. To support the ideas discussed in this paper, the author uses legal texts, international conventions, and official reports issued from national and international institutions.*

***Result and Conclusion:*** *In this paper, a comprehensive analysis of how IT has affected international relations has been presented. The researcher found that digital technology is considered a new international distribution of power and driving force in the social construction of war and peace. The paper also found that the war between Russia and Ukraine has proven that new technology is widely used in the conflict. The researcher also found that there is a binding legal framework to regulate the activities of the cyber domain. Moreover, new types of sanctions have been emerging internationally. During the conflict, new means of funding and new types of currency have been also been employed, which is considered a new challenge to international relations. The main finding of the paper is that new technology and cyberspace activities cannot be governed locally. The international community should involve civil actors in the governing and regulatory process of cyberspace.*

## 1 INTRODUCTION

In the recent past, information technology has had a profound impact on nearly every aspect of society, and international relations are no exception. Information technology has revolutionised the way countries communicate with each other, facilitating the spread of ideas and information.[1] It has also aided the flow of money, goods and people across borders.[2] As a result, international relations are increasingly shaped by the use of information technologies. Information technology has always had a major influence on global politics, economics, security, and culture. It has constantly shaped the way the global system works, the people involved, and how they interact with each other.[3] Its impact on international relations is no exception. Today, it has become a central part of diplomacy and the way countries interact with each other.[4] Technology and International Relations emphasise

1 Blayne Haggart, Kathryn Henne and Natasha Tusikov (eds), *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (Palgrave Macmillan 2019) doi: 10.1007/978-3-030-14540-8.

2 Mohamad Albakjaji, 'Cyberspace: The Challenge of Implementing a Global Legal Framework the Impacts of Time & Space Factors' (2020) 23 (4) Journal of Legal, Ethical and Regulatory 1.

3 Stefan Fritsch, 'Technological ambivalence and international relations' (E-International Relations, 24 February 2016) <https://www.e-ir.info/2016/02/24/technological-ambivalence-and-international-relations> accessed 14 February 2023.

4 Daniel R McCarthy (ed), *Technology and World Politics: An Introduction* (Routledge 2017) doi: 10.4324/9781317353836.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

the importance of leadership styles, domestic political agendas, and the relative weight of technologically driven countries in global affairs. The impact of these revolutions has been especially pronounced in the field of international relations.[5] Information technology has allowed countries to communicate with each other more easily than ever before.[6] This focus on technology highlights the ways in which different countries use information technology to shape the global system in their favour.

The Russian-Ukrainian war has proven that technology has greatly affected international relations, as technology has become an important factor in shaping them. For example, during the war, technology was used by Europe and the United States to impose new sanctions on Russia after proving that traditional and economic sanctions did not work.

It has been noted that the war proved that controlling cyberspace had a major role in making progress on the ground. It also became clear the role of the internet and social media in encouraging support for Ukraine. The neutrality that social media platforms used as an argument to defend their activities was abandoned. This paper will explore the ways in which information technology has affected international relations and explore how the traditional elements that governed international relations have changed.

The study aims to answer the following question: How did technology affect international relations, especially during periods of conflict, and especially during the Russian-Ukrainian war?

To answer this question, the researcher divided the work into three sections. The first will discuss new technologies as a spatial turn and paradigms of international relations. The second section will study the technology and the new international distribution of power. The third will cover the role of new technologies as a driving force in the social construction of war and peace. The case on the war between Russia and Ukraine will be explored in the fourth section where the aspects of new technologies' involvement in international relations will be explored.

## 2 NEW TECHNOLOGIES AS A SPATIAL TURN AND PARADIGMS OF INTERNATIONAL RELATIONS

In a rapidly globalising and digital world, the impact of information technology on international relations is more significant than ever before. The way in which nations communicate and interact with one another has been completely transformed by new technologies such as the internet, smartphones, AI and social media. Since the end of the Cold War, economic globalisation and the explosive growth of information communications technology (ICT) have dominated the political and corporate agenda, helping to define a new paradigm in which cooperation and competition must exist side by side among the most pragmatic nations and cultures.[7]

Another new area for security and diplomacy is cyber space, where today's rapidly advancing technologies enable a single person or small group to pose a serious danger to full-scale

5 Lucia Surdu (Pantea), 'Uncertainty: Strategic Thinking and International Relations in 21st Century' (2019) 11 Analele Universităţii Din Oradea, Seria Relaţii Internationale Şi Studii Europene 271.

6 John Krige and Kai-Henrik Barth, 'Introduction: Science, Technology, and International Affairs' (2006) 21 (1) Osiris, Global power knowledge: Science and Technology in International Affairs 1, doi: 10.1086/507133.

7 Amitav Acharya, 'Global International Relations (IR) and Regional Worlds A New Agenda for International Studies' (2014) 58 (4) International Studies Quarterly 647, doi: 10.1111/isqu.12171.

state apparatus.[8] The transition from the previously highly organized and regulated global environment to the new digital world is a paradigm shift.[9]

In the digital age the use of cyber-attacks or other forms of information warfare are increasingly possible. It is important to consider the implications of this technology on the practice of international relations when formulating theories, as it has the potential to fundamentally alter the way that states interact.

Recently, the term of spatial turn has emerged, which reflects the changing way in which the world is being experienced and focuses on space as a dynamic element in international relations. According to Baylis, technological advancement is critical in the establishment of a new guideline of international relations that is defined by networking, interconnection, and mutual interaction.[10] These shifts may be thought of as a series of "turns" that express the alteration of social life, science and research systems, and, most importantly, the current geopolitical arrangements from regional to global levels.[11]

Technological and spatial impacts on international relations are inseparably linked, as changes in one often reflect and amplify those in the other. For instance, the development of telecommunications and satellite technology has had a profound impact by facilitating global cooperation and the sharing of information. Such advances have enabled the establishment of a more fluid and interconnected world, which has led to new forms of conflict as well as cooperation.[12]

As a result, a new mode of specialisation became the deciding element in the creation of geopolitical tactics based on changeable operations at several scales ranging from the regional to the worldwide.[13]

In the context of international relations, technological and spatial change has been described as a "spatial turn." This refers to the growing emphasis on space in international relations scholarship, which reflects the changing way in which the world is being experienced.[14]

## 3 TECHNOLOGY AND A NEW INTERNATIONAL DISTRIBUTION OF POWER

The multifaceted effects of technology have an effect on international relations, their goals, and operational horizons.[15] Technology advancement encourages a shift in the organisation

8 Mohamad Albakjaji, and Jackson Adams 'Cyberspace: A New Threat to the Sovereignty of the State' (2016) 4 (6) Management Studies 256, doi: 10.17265/2328-2185/2016.06.003.

9 John Baylis, *The Globalization of World Politics: An Introduction to International Relations* (OUP 2020).

10 ibid.

11 Ken Booth and Toni Erskine (eds), *International Relations Theory Today* (2nd ed, Polity 2016). See also, Scott Burchill and others, *Theories of International Relations* (R Devetak and J True eds, 6th edn, Bloomsbury Publishing 2022).

12 Kalevi J Holsti, 'The Problem of Change in International Relations Theory' in *Kalevi J Holsti, Kalevi Holsti: A Pioneer in International Relations Theory, Foreign Policy Analysis, History of International Order, and Security Studies* (Springer 2016) 37.

13 Kate O'Neill, The Environment and International Relations (2nd edn, CUP 2017) doi: 10.1017/9781107448087. Due to digitally-mediated communication, there is a privacy conundrum when it comes to social communication and data transfer. Societies and political movements are the new way to participate in social and political life. In both situations, the successful mobilization of society depends on the propagation and utilization of information and the resulting communication technologies. Georg Sorensen, Jorgen Moller and Robert Jackson, I*ntroduction to International Relations: Theories and Approaches* (8th edn, OUP 2022).

14 Sorensen (n 15).

15 Mohamad Albakjaji, and Jackson Adams 'Cyberspace: A Vouch for Alternative Legal Mechanisms' (2016) 1 (1) Journal of Business and Cyber Security 10.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

of the international environment, changes the relationships between the major players in international relations, and increases the scope, acuity, and efficacy of transnational operations.[16] The impact of technology on modern international relations can be seen in many facets of social life and in the methodologies that govern them, such as the systems of institutionalisation and management of the global environment, connectivity, global collaboration, and interstate conflicts. Technology has shaped international relations through the ways in which it has influenced the way international institutions are set up, how information is shared and processed, as well as the methods of conflict resolution.

The role of technology in the distribution of power is also significant, as it has made possible the rise of new powers and lessened the influence of traditional players. For example, technology has helped to increase the economic might of China and other emerging economies, while reducing the relative military might of traditional powers. The diffusion of technology has also facilitated the spread of democracy and human rights as well as other forms of social progress.[17] Higher technological ability may be demonstrated in the methodical gathering, articulation, implementation, and adaption of knowledge, techniques, procedures, and processes, which is particularly indicative of the access to and use of power within the international system.

Technology is inextricably linked to power allocation amongst state and non-state actors in the international system as well as its ability and capabilities.[18] Although technology has had a significant impact on the way international relations are conducted, there are still many unanswered questions about the long-term effects of this new environment. For example, it is not yet clear how the diffusion of technology will affect interstate conflicts, or what will be the consequences of global networked societies for individual privacy and security.

Cyber-attacks are creating a challenge to international relations. The challenge of identifying the source of attacks, and the responsibility of the state for the attacks conducted by proxies, and the inability of states to immediately respond to such attacks are the main challenges facing the international community. Currently, the issues of cyberspace security, the behaviour of states in the cyberspace, and the respect of the international norms are at the top of the international community agenda. Nowadays, maintaining international peace is closely related to the way in which cyberspace activities are internationally governed.[19]

The way of dealing with cyber conflicts is still in the early stages. There are only some early international agreements that include some norms, which are on a voluntary base. The international rules governing traditional conflicts are well defined, such as the Geneva Convention, which aims to protect civilians during conflicts. It has been established that the rules that govern interstate cyber-attacks are still not well defined. Unlike traditional conflicts where the war takes place between two states while other nations silently watch, cyber-attacks may have an impact internationally.

In terms of institutionalisation, there are a number of changes that have been brought about by technology, such as the increasing use of social media and the spread of online

16 Baylis (n 11). See also, Zlatan Meskic, Mohamad Albakjaji, Enis Omerovic and Hussein Alhussein, 'Transnational Consumer Protection in E-Commerce: Lessons Learned From the European Union and the United States' (2022) 13 (1) International Journal of Service Science, Management, Engineering, and Technology 1.

17 O'neill (n 15).

18 Booth and Erskine (n 13).

19 'Ukraine Conflict: Digital and Cyber Aspects' (*Digital Watch, 2023*) <https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects> accessed 14 February 2023.

communities.[20] The way in which these new technologies are being used is indicative of a shift in the way international relations are conducted, from a top-down to a more participatory model. In addition, the way in which information is shared and processed has led to the development of new methods of conflict resolution, such as the use of cyber-attacks and online petitions. The increased connectivity of people throughout the world has also led to the emergence of new transnational organisations, such as multinational corporations and transnational criminal organisations.

Overall, technology and the distribution of power have had a significant impact on the way international relations are conducted. It has shaped the way international institutions are set up, how information is shared and processed, as well as methods of conflict resolution. Going forward, it is important to continue to study the long-term effects of this new environment on the way international relations are conducted.[21] Additionally, it will be necessary to explore new ways of implementing technology in order to ensure that it does not have negative impacts on the way international relations are conducted. Failure to do so could have significant consequences for the global system and distribution of power.

## 4 THE ROLE OF NEW TECHNOLOGIES AS A DRIVING FORCE IN THE SOCIAL CONSTRUCTION OF WAR AND PEACE

Technology has been a driving force in the social construction of war and peace. It has played a critical role in facilitating communication, transportation and trade, as well as influencing our ways of thinking. In the current era, new technologies are playing a significant role in facilitating the transfer of information and, as such, have affected the social construction of war and peace. One example is the use of drones.[22] Drones have been used extensively in conflicts around the world, from the War on Terror in Afghanistan to the Syrian Civil War. They have been used to carry out surveillance and airstrikes, making them a valuable tool in the fight against terrorism and insurgency. However, they have also been used in intra-state conflicts, notably in Sri Lanka. There, drones were used to carry out airstrikes in support of the Sri Lankan military, contributing to the escalation of the conflict. Drones have also been used in peacekeeping operations, most notably in the Democratic Republic of Congo, where drones carried out surveillance and airstrikes in support of the United Nations peacekeeping mission. In both cases, drones played a role in facilitating the transfer of information and, as a result, have had an impact on the social construction of war and peace.

Another example of how technology has influenced the social construction of war and peace is the use of social media. Social media has played a significant role in facilitating the spread of information and, as such, has had influence in this regard. One example is the use of Twitter in the Syrian Civil War. Twitter has been used to spread information about events in Syria, helping to shape public opinion about the conflict. In addition, it has been used to help organise protests and rallies, as well as to provide medical assistance to those affected by the conflict. Social media has also been used to spread propaganda from both sides of the conflict, helping to create an environment of misinformation.[23] In addition, the way platforms operate has changed during the conflicts. In this regard, Feldstein stated that:

20 Mohamad Albakjaji, Jackson Adams, Hala Almahmoud and Amer Sharafaldean Al Shishany, 'The Legal Dilemma in Governing the Privacy Right of E-Commerce Users: Evidence from the USA Context' (2020) 11 (4) International Journal of Service Science, Management, Engineering, and Technology 166.

21 Acharya (n 9).

22 Baylis (n 11).

23 Saul Bernard Cohen, Geopolitics: *The Geography of International Relations* (3rd edn, Rowman & Littlefield 2014).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

*The decision to finally drop the pretence of neutrality is ushering tech companies into a disorienting new era. No longer are they simply operating as neutral providers of technology. They are now making explicit value judgments regarding how governments use their platforms in wartime and what types of speech violate the bounds of hate, violence, and propaganda. These actions contradict prior content policies and indicate that companies are hastily rewriting their rulebooks—often in an ad hoc manner—in response to recent events.*[24]

For many years, social media has been criticised for its role in spreading disinformation and propaganda and it is clear that it has also played a significant role in shaping public opinion about conflicts. As a result, social media has played a role in contributing to the social construction of war and peace.

> *The concept of neutrality has changed. Before the Russia-Ukraine war, major internet platforms continued protecting themselves against governmental effort to hold them responsible for the content displayed on users' accounts. They keep arguing that they are not responsible for the content no matter how vile, and it is not possible to censor these platforms. However, these companies could not continue making such arguments.*[25] *With the outbreak of the war in Ukraine, the concept of neutrality no longer governs the work of these companies. YouTube announced that it had blocked more than 1000 Russian channels, and 15,000 videos. Facebook has followed suit and blocked access to official Russian outlets RT and Sputnik in the European Union. In addition, the ability of the Russian media to distribute information through Facebook has been banned. Big Technology companies such as Apple and Netflix, which suspended its service in Russia, have taken the same actions.*[26]

## 5 THE ASPECTS OF NEW TECHNOLOGIES INVOLVEMENT IN INTERNATIONAL RELATIONS: THE RUSSIAN INVASION ON UKRAINIAN TERRITORIES AS AN EXAMPLE

The Russian-Ukrainian war was not an ordinary or traditional war. Russia can no longer possess the keys to control the media because most Ukrainians have modern communication devices such as smart phones, which can connect to social media. So, all the outcomes of the invasion can be filmed directly without any delay and streamed internationally.

In this conflict, which is almost an international one, the question here is not what is new in this war, but rather the question is how to understand the dynamics of the modern media used in this conflict, which has become an additional force supporting the air, land and sea

24 Steven Feldstein, '4 Reasons Why Putin's War Has Changed Big Tech Forever: The Conflict Has Permanently Upended How the Major Platforms Do Business' (*Foreign Policy (FP)*, 29 March 2022) Argument. <https://foreignpolicy.com/2022/03/29/ukraine-war-russia-putin-big-tech-social-media-internet-platforms> accessed 14 February 2023.

25 ibid. The internet has led to the inclusion of new topics on diplomatic agendas, such as cyber security, data protection, internet governance, and artificial intelligence (AI) governance. This is significant as it shows that the internet is not just a tool that can be used to promote cooperation and understanding between different countries, but it can also be used to address some of the most pressing issues facing the world today. One risk is that internet-based diplomacy can be used to bypass traditional diplomatic channels. This can lead to misunderstandings and tension. Another risk is that internet-based diplomacy can be used to disseminate false information. For example, during the Ukraine crisis, Russian media used social media to spread disinformation about the situation in the country. See: James Curran, Natalie Fenton and Des Freedman, *Misunderstanding the Internet* (2nd edn, Rutledge 2016).

26 Feldstein (n 26).

forces.[27] The new aspect of this war is the harmony between traditional and modern media. As the broadcast of many pictures and videos via television - which are filmed by means of advanced technology devices such as mobile phones and others - are able to transfer the facts to the whole world. On the other hand, Russia has no ability to control it.[28]

Nowadays, the reports prepared by journalists are not the only means of communication and source of information. Internet users can also upload content and display it online through social media and share it with millions of users around the world.[29]

As mentioned earlier, in the era of cyber war, new technology is considered a supportive force for conventional arms. For example, during the war in Ukraine, Russia identified individual Ukrainian soldiers, designed fake contents, and sent it to the soldiers to persuade them to surrender. They even circulated an ai generated deep fake video of the Ukrainian leader asking Ukrainians to surrender. So, the term of electronic destruction has emerged, which has a greater impact on the infrastructure than traditional weapons of destruction. Therefore, blowing up a hospital or infrastructure is the same as hacking, and invading its network. Moreover, satellites were able to provide many photos of the Russian military forces invading Ukraine towards Kyiv. Digital technology plays a decisive role in the Russian-Ukrainian conflict, as providing a party with digital services, or withholding them from them, has a significant impact on the ground. When the war began in Ukraine, the battles were on various levels: on the ground, in the air, in the sea, in space, and online. A day before the outbreak of the war, Ukrainian government institutions and banks were the target of distributed denial of service (DDoS) attacks. The US and its allies have attributed these attacks to Russia and imposed sanctions on individuals supporting these attacks.[30]

After the increase in electronic attacks, many countries have become aware of the need for cyber armament to confront them. This urgent need has pushed states to maintain their cyber capabilities to protect themselves against any malicious activities that take place within cyberspace, which is considered the fifth military domain (after land, sea, air, and space). The issue of attributing cyber-attacks to a specific country is challenging as well, where cyber proxies, which have an important role in increasing the risk of escalation, usually conduct these attacks.

On other hand, the American and Russian nuclear arsenal still contains the potential threat of turning any conflict between these powers into a new world war. For this reason, the USA refused to impose a no-fly zone over Ukraine. Instead of imposing such a zone, NATO provides Ukraine with new types of weapons such as missile systems and drones. Although Russia invaded Ukraine, it has been unable to penetrate into vast areas since the outbreak of the war. The use of new technology in the war, such as the use of drones, has proven the Ukraine's proficiency in the war.[31]

Financial technology (fintech) has its impact on the Russian economy as well. The Russian economy has been severely affected, as represented by the shutdown of Russian banks in Europe and America, as well being deprived of access to the SWIFT payment system, which

27 Katharina Niemeyer and others, 'The Russian Invasion Shows How Digital Technologies Have Become Involved in All Aspects of War' (*The Conversation*, 28 March 2022) <https://theconversation.com/the-russian-invasion-shows-how-digital-technologies-have-become-involved-in-all-aspects-of-war-179918> accessed 14 February 2023.

28 ibid.

29 ibid.

30 Ukraine Conflict (n 21).

31 Kelsey D Atherton, 'How Technology, Both Old and New, Has Shaped the War in Ukraine So Far' (*Popular Science*, 7 April 2022) <https://www.popsci.com/technology/technology-russia-ukraine-war> accessed 14 February 2023.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

eventually led to the closure of the stock market in the country. In the same vein, Russian investors were affected. For example, Russian importers could no longer pay the price of goods imported from America.[32]

## 5.1 The absence of a binding legal framework to regulate the activities of the cyber domain

The Russian-Ukrainian conflict revealed that activities that take place in cyber space are not yet governed by a legal framework at the international level. This made countries unbound by any legal scope and as a result, the sovereignty of other countries can be easily breached when conducting activities in cyberspace, which is considered cross border activity. The UN adopted some cyber agreements which established an international framework, but on a voluntary base.

Both countries, Russia and Ukraine signed these agreements. This framework includes some norms, which confirm that cyberspace should be governed by international law, and international humanitarian law should be applied during armed force.

In addition, participating states of the Organization for Security and Co-operation in Europe (OSCE) – including Russia, Ukraine, Belarus, the USA, and other European countries – have agreed on a set of voluntary confidence-building measures (CBMs). CBMs include consultations to reduce the risks of misperception, escalation, conflict, and use the OSCE as a platform for dialogue.[33]

Although, there are international rules, such rules are non-binding and of a voluntary nature. They do not provide for penalties in the event that countries violate such rules, but rather they have become a code of conduct.

## 5.2 The Russian-Ukrainian war and the emergence of a new type of sanctions at the international LEVEl

Technology has had a great impact on international relations. Previously, economic and military sanctions were the procedure taken by the international community against a country when it violated its international obligations. Technological development has led to the emergence of new types of sanctions internationally.

In addition to the economic sanctions imposed by the US, EU, etc., which affected Russian imports, the US and its allies announced a set of digital sanctions. Cloud computing centres, high-performance computers, aviation, defence technologies, and oil-refining machinery all require regular replacements and upgrades of microprocessors, controllers, sensors, and mechanical parts. Blocking such technology may lead to paralysis of these services, and will eventually have a significant impact on weakening military access.

32 Emily Gersema, 'Technology, Nuclear Power are Driving Issues in the Russia-Ukraine War: USC Experts Discuss How Tech-Driven Globalization and Energy are Front and Center in Russia's War on Ukraine' (*USC News*, 4 March 2022) <https://news.usc.edu/197476/technology-nuclear-power-are-driving-issues-in-the-russia-ukraine-war> accessed 14 February 2023.

33 Ukraine Conflict (n 21).

### 5.3 Conflict and Technology: The emergence of Digital Currency as a challenge to international relations

Crypto currencies have become a decisive factor in the conflict. Both countries have increasingly used these currencies to overcome the financial and economic crises in the region.

In Ukraine, significant progress has occurred. A new regulation has been adopted on digital assets. In addition, Ukraine has recognised bitcoin and other cryptocurrencies have played a significant supporting role during the conflict.

Previously, during periods of conflict, traditional methods of financial transfers were used to support the invaded country, such as bank transfers, support for its exports, and other methods. Nowadays, new supportive procedures have been adopted internationally. An example is GoFundMe, a crowdsourced fundraising app where donors can send cryptocurrencies to help Ukraine. Moreover, new technologies have been leveraged, such as Solana, Polka Dot, and NFTs in order to facilitate donation. More than 33 million dollars were collected during the first week.

Ukrainian refugees in neighbouring countries who have traditional bank accounts were not able to access their assets whereas people who have digital accounts and assets were able to access their assets internationally. This gave cryptocurrencies transboundary international value during the crisis.[34]

Russia, which was opposed to cryptocurrencies, has started to use them and has adopted a new draft on a central bank digital currency (CBDC) and new regulations for other digital currencies, despite the opposition of the Central Bank.[35]

Although cryptocurrencies have a good impact in terms of supporting the invaded state, they create a challenge to international relations because governments currently have only a limited ability to control money transfers as they will be sent from 'nowhere' to 'nowhere'. So, most international agreements on the control of the money transfer no longer work. A good example of this is that Russia used cryptocurrencies to support its commercial activities internationally. In addition, some other countries which are under strict financial sanctions, such as Iran, have used them as well, despite the strict financial embargo. In a 'war economy', cryptocurrencies can be used to circumvent strict sanctions on the banking system, crowdfunding, and other financial activities.[36]

## 6 LEGAL GAPS IN LEGAL FRAMEWORKS WHEN ADDRESSING THE IMPACT OF DIGITAL TECHNOLOGIES IN INTERNATIONAL RELATIONS

Digital technologies have quickly advanced and are now widely used, posing significant challenges for international law and diplomacy. There are a number of legal gaps in current legal systems that must be filled in the case of the conflict between Russia and Ukraine. The resolution of the conflict and the capacity of international organisations to adequately address the problems presented by digital technology can both be significantly impacted by these disparities.

The absence of precise and widely recognized guidelines on the use of digital technology

34 ibid.
35 ibid.
36 ibid.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

in conflict is one of the major legal gaps in this field. Although the use of cyberattacks in conflicts throughout the world is on the rise, there is currently no comprehensive international legal framework that governs this practice. As a result, it is difficult for nations to protect themselves against cyberattacks and for international organisations to properly respond to instances of cyberwarfare. This leads to confusion and misunderstanding about what is permitted and what is forbidden.

The rise of cyber-crime presents a challenge for the application of international laws and its principles. According to the United Nation Charter's Article 2 clause 4, countries are forbidden from using cyber strength against other countries, granting each state sovereign control over their own territory and digital infrastructure. However, states are still responsible for preventing the use of their digital infrastructure for illegal activities that impact other states.

International courts have granted states the right to respond to cyber-attacks if they pose a serious threat to their essential interests. This right to self-defence is based on Article 51 of the United Nation Charter and customary international law, allowing a country to use strength to guard against armed attacks, including cyber-attacks causing death, injury, or significant damage.

There are several areas of ambiguity in international law regarding cyber-crimes, particularly in the ICJ's Congo ruling and Wall consultative view, which seem to limit the right of self-defence to instances of cyber-attacks that meet the criteria of "armed attacks" done by countries leading to significant harm.

Protocol I defines an "attack" as an "act of violence." There is a general understanding that this definition can encompass cyber operations that result in physical harm or injury. However, it is unclear whether the protection afforded under this definition applies to cyber-attacks that cause significant economic damage to civilians and civilian targets, even if no physical damage occurs.

Global law is uncertain about the identity of cyber attackers, and it is often assumed that countermeasures can only be taken by victim states if the attacker is another state. However, this assumption may not hold true if the attacker is a non-state actor, such as an individual or a transnational terrorist group. In such cases, victim states may extend their self-defence measures to include these non-state actors. However, proving the connection between the non-state actor and the state responsible for the attack is difficult, as attackers can conceal their identity and locality by using what is termed the "Dark web".[37]

Once more the legislation does not detail if countries must supervise their own digital systems for any illegitimate use and implement procedures to avert such misappropriation. To illustrate, Article 8 of the Draft Articles adopts a restricted perspective on a state's responsibility for actions performed by private entities, where the state is legally accountable for actions carried out by these entities if they act under the state's guidance, supervision, and direction.

Therefore, HongjuKoh maintained that legal structures globally must be more incorporating:[38]

"These rules are designed to ensure that states cannot hide behind putatively private actors to engage in conduct that is internationally wrongful." (p.6)

Moreover, international courts have taken a restrictive approach towards defining the

37 The Dark Web is a collection of websites that are publicly visible, but hide the IP addresses of the servers that run them. Thus they can be visited by any web user, but it is very difficult to work out who is behind the sites. And you cannot find these sites using search engines.

38 Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal online 1 <https://harvardilj.org/2012/12/online_54_koh> accessed 14 February 2023.

concepts of "direction" and "control." For example, in the Nicaragua versus USA case, Nicaragua claimed that there was a connection between the USA and cyber-attacks carried out by rebellious groups in Nicaragua. However, the ICJ downplayed the role of the U.S.A even though the group was provided with financial and military support. Thus, providing training and weapons to rebel groups is evidence of a relationship between proxy players and the supporting country, while simply supplying funds and equipment does not imply a country's involvement in using force or go against Article 2(4) of the United Nations Charter. This has faced criticism from various scholars, including Margulies[39], who noted that the International Court of Justice (ICJ) has expressed these conditions in its definition of what it referred to as an "effective control" test. He added that although the phrase "effective control" might suggest actual control to listeners in the United States, the ICJ's usage of the term implies a form of control that is more precise and all-encompassing. Additionally, he stated that the phrases concerning control and direction outlined in the draft documents were vague, and he criticised the International Criminal Tribunal for the former Yugoslavia (ICTY) for its belief that a determination of state accountability necessitated formal involvement in the preparation and overseeing of military actions.

Another legal gap is the haziness around jurisdiction and the extraterritorial application of national laws in the digital world. This makes it difficult for states to hold individuals and entities accountable for negative conduct committed via digital technologies. For instance, it could be difficult for Ukraine to take legal action against Russian individuals or groups who intervene in its domestic affairs digitally. The fast advancement of digital technology has also brought forth new challenges for the defence of human rights in the modern day.[40] Although human rights are recognised in international law, there are still substantial legal gaps that prevent the protection of these rights in the digital sphere. For instance, it is challenging for nations to safeguard the privacy of their citizens and for international agencies to effectively address abuses of privacy rights since there is currently no agreed-upon concept of privacy in the digital era.

In order to address the effect of digital technologies on international relations, there are not enough efficient international collaboration institutions.[41] Even though there are many international organisations and conferences that deal with issues linked to digital technologies, there is still a need for a more efficient and coordinated response to the problems that these technologies cause. For instance, it could be challenging for Russia and Ukraine to work together to investigate cybercrimes that are perpetrated utilizing digital technology.

Considering the significant gap that exists, it is important for international institutions and governments to work together to develop new legal frameworks and mechanisms to address these challenges and to ensure the protection of human rights in the digital age.

Individuals play a crucial role in cyber activities and therefore should take a prominent position in the regulation of cyberspace. The management and regulation of internet and digital technologies should be grounded in human rights law.

Advocates of the conventional perspective advocate for the application of the Cyber Westphalia system, which governs international relations by prioritising state sovereignty over individuals. This would allow each state to establish its own online borders. Demchak and

39 Peter Margulies, 'Sovereignty and Cyber-Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 (2) Melbourne Journal of International Law 496.

40 Jawahitha Sarabdeen, 'Protection of the Rights of the Individual When Using Facial Recognition Technology' (2022) 8 (3) Hylion 1, doi: 10.1016/j.heliyon.2022.e09086.

41 Niemeyer and others (n 29).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Dombrowski[42] posited that the contemporary Westphalian has been explained by territory, independence, governance, and mutual understanding in accordance with traditional international relations theory. They noted that while telecommunication companies and regulatory agencies may adopt different approaches to defining a nation's cyber borders, each will determine what is and is not considered part of the state in cyberspace.

According to Kulesza and Balleste[43], the idea of the "cyber Westphalian age" is flawed because it rests on the notion that a nation can ensure its security by creating online jurisdictions. Nevertheless, in an era of globalisation, where the globe has become like an interconnected village, the traditional idea of independence that forms the backbone of the Westphalian system needs to be replaced with inventive concepts like shared sovereignty. The authors criticise the notion of the "good fence" concept in the cyber Westphalian idea for not acknowledging the reality of a world without borders and the science that shows the universe has no boundaries.

Proponents of cyber Westphalia believe that it's possible to establish boundaries in cyberspace because it's a man-made technology.[44] However, this perspective fails to consider international human rights agreements, for instance the Universal Declaration on Human Rights (1948) and the International Covenant on Civil and Political Rights (1966). It overlooks the role of the internet in enabling other privileges, for instance education, civil and political privileges.[45] Imposing restrictions or censorship in the online world would therefore infringe upon human rights, particularly freedom of speech. Kulesza and Balleste[46] also pointed out that creating borders in the digital realm would hinder the free exchange of information and result in a less interoperable network, where information would be limited and controlled through narrow gateways.

According to Duplessis[47], the state should establish a new approach to enable private parties to have a say in regulating cyberspace, through the use of "soft law". This type of regulation is a new form of social control in the digital world. The concept of cooperation in decision-making has a rich history, starting from the period of "jus gentium" and later becoming the "law of nations", which was practised in the Roman Empire.[48] Soft laws are known for their ease of development, practicality, and adaptability.[49] The World Summit on the Information Society[50] emphasised the significance of this collaboration, defining it as the creation of an inclusive information society through partnerships and collaboration with administrations, the private sector, public spheres, and global establishments. The 2005 Tunis Agenda of WSIS further described the steps for the development of Internet governance, which involves the

42 Chris C Demchak and Peter J Dombrowski, 'Cyber Westphalia Asserting State Prerogatives in Cyberspace' (2014) spec (on cyber) Georgetown Journal of International Affairs 29.

43 Joanna Kulesza and Roy Balleste, 'Signs And Portents In Cyberspace: The Rise Of Jus Internet As A New Order In International Law' (2014) 23 (4) Fordham Intellectual Property, Media & Entertainment Law Journal 1311.

44 Demchak (n 44).

45 Frank La Rue, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue : addendum' (*UN*, 27 May 2011) <https://digitallibrary.un.org/record/706200> accessed 14 February 2023.

46 Kulesza (n 45).

47 Isabelle Duplessis, 'Le vertige et la *soft law*: réactions doctrinales en droit international' (2007) Hors-série Revue québécoise de droit international 245. Isabelle Duplessis, 'Le vertige et la soft law: réactions doctrinales en droit international' (2007) Hors-série Revue québécoise de droit international 245.

48 Kulesza (n 45).

49 Albakjaji (n17).

50 Declaration of Principles : Building the Information Society: a global challenge in the new Millennium WSIS-03/GENEVA/DOC/4 (12 December 2003) <https://digitallibrary.un.org/record/533621> accessed 14 February 2023.

participation of all groups involved in the growth of the Internet, including state authorities, civil society, and the business sector.[51]

This method of establishing soft law alone is not enough to incorporate global peer agreement into country's legal frameworks. However, global organisations must acknowledge the pronouncements made by the cyber community and motivate countries to adopt these laws at a national level. For example, child pornography was deemed unacceptable by most cyber societies and privacy guidelines were established by major internet service suppliers without a global consensus on personal data protection. Thus, the process of adopting soft laws is similar to the creation of international customary law. The International Court of Justice requires two elements for international customary law to exist: a uniform practice among state authorities and a belief by national authorities that the specific behaviour portrayed in this practice is familiar to other countries as having legal force.

The currently available international frameworks do not permit the cyber-community to play a role in the decision-making process. However, global communities must consider the uniform practices agreed upon by the cyber-community and attempt to implement them both internationally and nationally. To strengthen this argument, Albakjaji and Adams[52] have advocated for the involvement of explicit stakeholders in the development of internet regulation and control of cyber actions, emphasising the importance of soft laws.

## 7 CONCLUSIONS

International relations have been shaped by the rise of Information Technology (IT). In this research paper, a comprehensive analysis of how IT has affected international relations has been presented. The war between Russia and Ukraine as a case study has been used to analytically discuss how new technology has recently been involved in all the aspects of the war. The researcher found that new technology is considered an important factor during both peace and war. Thus, digital technology could be effectively involved in international relations where new aspects have emerged which did not exist before the war, such as the use of new sanctions based on technology, as it has become evident that traditional sanctions are of limited use. Moreover, the widespread use of digital currencies during the war proved that the international community is unable to control these types of financial transactions, which may sometimes be illegal. The current paper has also put a spotlight on the fact that the internet and the social media have played a decisive role in circulating information internationally, and at a time where states are unable to do it without using digital technology. This has led the international community to recognise and emphasise the role of the new technology and heavily rely on it to support Ukraine. This makes digital technology platforms a moving wheel in mobilising public opinion to support the views they wish to pass at the international level. This is also considered a new challenge for international relations, which did not face such a challenge before.

To overcome these challenges, new rules should be adopted internationally. These legal measures may be crucial in reducing the negative effects of digital technology on the ongoing conflict between Russia and Ukraine. For instance, it might assist in lowering the danger of cyberattacks and other negative uses of digital technology by defining the responsibility of nations in cyberspace. In a similar vein, it might contribute to preventing the use of digital technology to meddle in the internal affairs of other nations and aid in respecting the sovereignty of other states in cyberspace by encouraging responsible state conduct.

51 Tunis Agenda for the Information Society WSIS-05/TUNIS/DOC/6(Rev1)-E (18 November 2005) <https://digitallibrary.un.org/record/565827> accessed 14 February 2023.

52 Albakjaji (n17).

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

In the context of the conflict between Russia and Ukraine, there are a number of suggested policies and laws that might serve as a framework for addressing how digital technology affects international relations and assists in avoiding conflicts and safeguarding civilians from harm. The adoption of both cyber warfare and International Humanitarian Laws, as an example, would resolve the legal issues and guarantee that international humanitarian rules apply to cyber warfare - and that any acts conducted during such conflicts are compliant with the law of armed conflict. Additionally, international criminal law has to be strengthened. It is crucial to establish clear norms and standards for the use of digital technology in international relations, including the application of international criminal law to serious cyber-crimes, such as hacking and cyber-espionage. It is also recommended to establish laws on state responsibility for cyber-attacks. Such laws must address this issue, including the principle of state responsibility for acts of cyber-crime and the duty to investigate and prosecute cyber-crime. Further, addressing the legal challenges would require data privacy and cybersecurity laws. To safeguard individuals against the negative effects of digital technology and to guarantee that its usage does not violate privacy and civil rights, the international community must endeavour to develop universal laws for data privacy and cybersecurity. The establishment of a treaty system for cyber security is also recommended. A framework for international cooperation in addressing cyber threats, clear rules and norms for the use of digital technology in international relations, and assurance that state actions in cyberspace adequately reflect international law all require the establishment of an international treaty regime for cyber security.

The article also found that, because of the characteristics of the internet, it is not possible for one state alone to regulate this virtual world. Considering that the internet is a stateless space, the study has proven that national and international laws have become outdated and ineffective in managing it.

Consequently, all attempts to govern it internally will be doomed to failure because technological and digital developments are proceeding at a much faster pace than the traditional legislative and regulatory frameworks.

Therefore, the researchers recommend that the best way to govern the Internet should be through international cooperation between states on the basis of a shared sovereignty. The international community should involve civil actors in managing and regulating online activities. This includes cooperation with people who work in the field, such as engineering, academic, users, and law practitioners because they are well qualified in the area of cyberspace and new technology. They can easily adopt new and flexible soft roles when facing emerging circumstances which need immediate solutions.

## REFERENCES

1. Acharya A, 'Global International Relations (IR) and Regional Worlds A New Agenda for International Studies' (2014) 58 (4) International Studies Quarterly 647, doi: 10.1111/isqu.12171.
2. Albakjaji M, and Adams J, 'Cyberspace: A New Threat to the Sovereignty of the State' (2016) 4 (6) Management Studies 256, doi: 10.17265/2328-2185/2016.06.003.
3. Albakjaji M, and Adams J, 'Cyberspace: A Vouch for Alternative Legal Mechanisms' (2016) 1 (1) Journal of Business and Cyber Security 10.
4. Albakjaji M, Adams J, Almahmoud H and Al Shishany AS, 'The Legal Dilemma in Governing the Privacy Right of E-Commerce Users: Evidence from the USA Context' (2020) 11 (4) International Journal of Service Science, Management, Engineering, and Technology 166.
5. Albakjaji M, 'Cyberspace: The Challenge of Implementing a Global Legal Framework the Impacts of Time & Space Factors' (2020) 23 (4) Journal of Legal, Ethical and Regulatory 1.

6. Atherton KD, 'How Technology, Both Old and New, Has Shaped the War in Ukraine So Far' (*Popular Science*, 7 April 2022) <https://www.popsci.com/technology/technology-russia-ukraine-war> accessed 14 February 2023.
7. Baylis J, *The Globalization of World Politics: An Introduction to International Relations* (OUP 2020).
8. Booth K and Erskine T (eds), *International Relations Theory Today* (2nd ed, Polity 2016).
9. Burchill S and others, *Theories of International Relations* (R Devetak and J True eds, 6th edn, Bloomsbury Publishing 2022).
10. Cohen SB, *Geopolitics: The Geography of International Relations* (3rd edn, Rowman & Littlefield 2014).
11. Curran J, Fenton N and Freedman D, *Misunderstanding the Internet* (2nd edn, Rutledge 2016).
12. Demchak CC and Dombrowski PJ, 'Cyber Westphalia Asserting State Prerogatives in Cyberspace' (2014) spec (on cyber) Georgetown Journal of International Affairs 29.
13. Duplessis I, 'Le vertige et la *soft law*: réactions doctrinales en droit international' (2007) Hors-série Revue québécoise de droit international 245.
14. Feldstein S, '4 Reasons Why Putin's War Has Changed Big Tech Forever: The Conflict Has Permanently Upended How the Major Platforms Do Business' (*Foreign Policy (FP)*, 29 March 2022) Argument. <https://foreignpolicy.com/2022/03/29/ukraine-war-russia-putin-big-tech-social-media-internet-platforms> accessed 14 February 2023.
15. Fritsch S, 'Technological ambivalence and international relations' (*E-International Relations*, 24 February 2016) <https://www.e-ir.info/2016/02/24/technological-ambivalence-and-international-relations> accessed 14 February 2023.
16. Haggart B, Henne K and Tusikov N (eds), *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century* (Palgrave Macmillan 2019) doi: 10.1007/978-3-030-14540-8.
17. Holsti KJ, 'The Problem of Change in International Relations Theory' in Holsti KJ, *Kalevi Holsti: A Pioneer in International Relations Theory, Foreign Policy Analysis, History of International Order, and Security Studies* (Springer 2016) 37.
18. Koh HH, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal online <https://harvardilj.org/2012/12/online_54_koh> accessed 14 February 2023.
27. Krige J and Barth KH, 'Introduction: Science, Technology, and International Affairs' (2006) 21 (1) Osiris, Global power knowledge: Science and Technology in International Affairs 1, doi: 10.1086/507133.
28. Kulesza J and Balleste R, 'Signs And Portents In Cyberspace: The Rise Of Jus Internet As A New Order In International Law' (2014) 23 (4) Fordham Intellectual Property, Media & Entertainment Law Journal 1311.
29. Margulies P, 'Sovereignty and Cyber-Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 (2) Melbourne Journal of International Law 496.
30. McCarthy DR (ed), *Technology and World Politics: An Introduction* (Routledge 2017) doi: 10.4324/9781317353836.
31. Meskic Z, Albakjaji M, Omerovic E and Alhussein H, 'Transnational Consumer Protection in E-Commerce: Lessons Learned From the European Union and the United States' (2022) 13 (1) International Journal of Service Science, Management, Engineering, and Technology 1.
32. Niemeyer K and others, 'The Russian Invasion Shows How Digital Technologies Have Become Involved in All Aspects of War' (*The Conversation*, 28 March 2022) <https://theconversation.com/the-russian-invasion-shows-how-digital-technologies-have-become-involved-in-all-aspects-of-war-179918> accessed 14 February 2023.
33. O'Neill K, The Environment and International Relations (2nd edn, CUP 2017) doi: 10.1017/9781107448087.
34. Sarabdeen J, 'Protection of the Rights of the Individual When Using Facial Recognition Technology' (2022) 8 (3) Hylion 1, doi: 10.1016/j.heliyon.2022.e09086.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

35. Sorensen G, Moller J and Jackson R, Introduction to *International Relations: Theories and Approaches* (8th edn, OUP 2022).

36. Surdu (Pantea) L, 'Uncertainty: Strategic Thinking and International Relations in 21st Century' (2019) 11 Analele Universității Din Oradea, Seria Relații Internationale Şi Studii Europene 271.