



Reshaping International Relations in the Age of Digital: Strategies and Implications

Amine.boulenouar

abou bekr belkaid - Tlemcen,, (Algeria)

amine.boulenouar@univ-tlemcen.dz

Abstract ;

In the contemporary landscape of international relations, digital technologies have emerged as a pivotal force reshaping diplomatic practices, state interactions, and global governance. This paper explores the strategies adopted by nations to navigate the complexities introduced by digitalization, including cybersecurity, digital diplomacy, and the influence of social media on public opinion and policy-making. It examines the implications of these strategies on power dynamics, sovereignty, and international cooperation. By analyzing case studies of digital initiatives and their impact on bilateral and multilateral relations, the paper highlights both the opportunities and challenges posed by the digital age. Ultimately, it argues that a robust framework for digital governance is essential for fostering sustainable international relations in an increasingly interconnected world

Article info

Received

January 19.2025

Accepted

March 04.2025

Keyword:

- ✓ Digital Age; International Relations;
- ✓ Digital Diplomacy;
- ✓ Cybersecurity;
- ✓ Digital Governance ;
- ✓ Global Governance.

1. *Introduction*

'The Digital Age' presents a paradox of depth and diversity with respect to its penetration into various levels, domains, and dimensions of human existence. Yet, glancing through half a century of texts on statecraft and diplomacy, hardly any language – operational, policy, or intellectual – could be found in international relations that has been shaped or has adapted to capture this seismic transformation of traditional diplomatic practices, interstate and intersociety relations, intrastate-society and society-society interactions. The rapid evolution of digital technologies is not only enhancing the possibilities for innovation and development but also profoundly altering the way in which work is organized, transactions are made, service delivery is mediated, enterprises are created, and social interactions are conducted and represented¹. Alongside the ambiguities and controversies enveloping these innovations, these transformative potentialities have profound implications for the challenges of global governance, local resource management, and regulatory equilibrium².

Within international relations, the central conceptual, theoretical, and operational quandaries of this new paradigm have hitherto remained malnourished. Empirically sound analytical insights are,

however, critical for understanding emergent means, modalities, and trends that could complement or subvert established state and interstate practices in the conduct of international relations. The ability to innovate, absorb, adapt, and co-evolve in digital content and form is increasingly conflated with – and is at the core of – power. Every major conceptual mapping of global power shows an orientation toward adjusting to and from within digital enablement. Countries and regions alive and vibrant in digital adaptation would not only get ahead but would also dominate outcomes in contests and rival centers. The question, therefore, is if and why concepts, doctrines, and strategies adapted into state diplomacy and digital governance are necessary; and what implications may be visualized from a lack of – or from – composite adaptation in the conduct of international relations.³

The problem:

How are digital technologies transforming diplomatic practices and state interactions in the context of international relations?

2. *The Impact of Digital Technologies on International Relations*

The impacts of digital technologies are multi-faceted. In terms of diplomacy, innovations such as the internet have 'democratized' state-based activities in international relations, with citizens and

non-governmental actors having access to information and the ability to participate in forums of public diplomacy on scales previously unforeseeable. Those involved in politics also have access to citizen and crowd sentiment, using social media interactions to make promotional claims or to identify dangerous trends in online public opinion. The communicative aspects of digital technologies are crucial. The way that information is communicated to both domestic and foreign publics about the actions, intentions, norms, and ideas of others directly and indirectly impacts national security and state legitimacy⁴. The relationship between digital and the transmission of information is also twofold. Innovations in digital communications increase the ability of states and their actors to transmit information to foreign publics, but also increase the volume and channels by which others can do so. At the same time, there is a dark side to digital. The spread of 'fake news' or 'deepfakes' shows how digital communication can also be used for harm. This ambivalence towards digital technology means that states are faced with a number of barriers and opportunities to enhance their soft power tools.⁵ Numerous states have begun to recognize the benefits of utilizing digital technologies as part of public diplomacy to benefit their reputations, though more investments could be made in this field.

Consequently, states have been advancing 'digital diplomacy' and their support for technological innovation, but a number of states have also begun to use diplomatic tools in the field of cybersecurity, impacting negatively the information available that can engage in diplomatic discourse via digital means.⁶ These three different elements are separate and unique, and should not be treated as a logical consequence of one another.

2.1. Cybersecurity Threats and Challenges

The pervasive digitalization of government, business, and society has led to new vulnerabilities that can be exploited by malicious cyber threats. Growing connectivity also means that cyberattacks have the potential to be very effective in causing harm. State actors pose a more significant threat than other attackers. Some states have used cyber weapons to provoke or escalate a conflict, and others may do so in the future. In particular, states with clearly articulated anti-status quo foreign policies are likely candidates to strike. But even actors that believe their position is being undermined are likely to be induced. It is primarily the capabilities of a state and not its intentions that determine the potential threat. A smaller number of states will dominate the global battle of the digital era, much as the relatively few states ruled the waves of previous eras.⁷

The United Nations described the measures necessary to reassert these trends. The methodology for prevention, response to, and consequences of major cyber incidents involves cybersecurity requirements, trust, and protecting networks. Because the strategy is based on a capacity building concept, it is a collection of best practices and learning resources, such as curriculum and training. To assist companies in keeping their networks secure, these policies must also be backed up by global norms, adhering countries. The number of policies from international organizations is growing. The Code of Conduct for International Cyberspace establishes recommended best practices for bodies such as the European Union⁸ and the Organization of American States. The strategy of trust includes confidence-building announcements as well as working arrangements and centers of information that encourage other stakeholders to exchange information in an emergency. Information is usually shared with governments, including industry, but other agreements are multisectoral. Regular information sharing is provided by both the administration and the National Council on Cybersecurity. It assists security experts from private industry and the government in increasing their knowledge, as well as in defending against and responding to cyber threats.⁹

2.2. Digital Diplomacy and Soft Power

Regarding the significance of digital platforms, the governments of states employ social media to communicate and engage with foreign publics. As most users are individuals rather than institutions, social media has become a critical environment wherein states can influence foreign populations and also form relationships with them. In this way, the fundamental purpose of digital diplomacy is to create a positive image of the state in order to foster admiration and, by extension, policy compliance. By doing so, social media platforms are a means to soft power¹⁰. This is increasingly the determination of how online influence can translate to foreign policy victories. The strategies of likable and linkable communication, via charismatic leadership, feel-good content, and ultimately, widespread relatability in digital engagement are being analyzed. Case studies are beginning to appear on this type of nation branding and aspirational lifestyle approach; certain governments are effective practitioners of this approach, driving their online influence to desirable foreign policy outcomes.

The challenges of digital diplomacy and social media warrant more careful engagement with this contemporary phenomenon. Misinformation will always be a threat at any point in time at which a

source of 'the truth' gives way to polyphony and relativism.¹¹ The rush for social media celebrities to be chosen as influencers in an era where more and more accounts can be purchased relates to international relations in attracting foreign tourists. Correspondingly, the question of regime authenticity currently inflects research on the involvement of diplomats on all social media. One crucial question is how accountable a public must their regime be in order to be effectively consular and representative in a digital age? It is clear that nation-states are increasingly willing to mobilize resources in the service of image management abroad, regardless of the answer. Public diplomacy in the context of digital can be considered the co-product of two powerful factors: the intrinsic need for foreign contact and trust in constrained physical contact situations, and the fundamental societal shift towards digitization more increasingly disclosed by public health emergencies¹².

3. Strategies for Adapting to the Digital Age

The first step for the world, and each state, is to identify the challenges faced in and by cyberspace¹³. These digital threats might come from states, criminals, terrorists, or hackers; they may have differing objectives and biggest targets – from paralyzing the internet in a state to spreading chaos and uncertainty to

targeting nuclear power plants or personal data. When identification of problems is possible, it becomes easier to address them. For instance, multilateral agreements, coherent international rules of the game, both in hard – keeping the networks free and soft power performances, along with the implementation of robust corporate social responsibility, are required. This thinking includes the position, priority, and institutional priority for all the actors: states, international enterprises, and governmental bodies. Additionally, digital resources need to be mobilized to provide digital inclusion – those without it will miss out on some human rights and on the prosperity-based maintenance objective too¹⁴. To this end, regulations of the new products and services need a balance of two fundamental needs: security and unrestricted room for tech innovation. Furthermore, it also leads to some basic national strategic planning regarding the priority and the needs of the prioritization in the overall national sector-based long-term planning. Governance instruments will need to be efficient, with high legal credibility and the proper globally trusted regulatory institutions given the highly daring and rapidly changing global trends. Even these institutions will need to demonstrate a high degree of intersectional digital competence and capillarity in transferring it whenever necessary.

3.1. Enhancing International Cooperation in Cyberspace

The urgency and complexity of global digital governance require enhanced international cooperation. States with different interests and diverse domestic and regional systems are reluctant and often unable to find a consensus within existing organizations. At the same time, states and international organizations share a vision to maintain the global free, open, and secure digital system almost in the same form it was before. However, this "most favored" nature of the egalitarian regime of the Global Wide Web is not taken for granted by the huge economic and military power of the major actors. International organizations offer platforms to launch dialogue without obligation, to study national interests, and to facilitate incentives among states.¹⁵

In the area of cybersecurity and developing rules of the road in cyberspace, international cooperation is necessary yet rare. Although cyberspace is a globally shared domain, the sovereignty of the state, ranging from the dimension of the "thing" to the "power," results in the autonomous jurisdiction of the state. In principle, the state is a natural player in cyberspace. Despite this fact, a variety of joint initiatives have been developing cybersecurity as a global regime of collective security¹⁶. These regimes intend to support international

cooperation¹⁷, such as the criteria for sovereign intervention. Cybersecurity regimes are both open for membership and deepen their cooperation in a liberal manner.

The first open initiative on cybersecurity is drafting. Developing countries were eager to create a more effective and relevant approach to address cyber peace, sharing their capacity plans for peace, and pursuing shared economic development. Norms play a key role in any system of international cooperation. To the degree that states take into account the interests of others, they are more likely to design, empower, and enforce regimes that improve international cooperation to better serve their long-term goals and objectives¹⁸. Norms shape costs and benefits relative to behavior. By coordinating expectations, norms can help reduce transaction costs, including measurement, information processing, policy negotiation, and enforcement. High transaction costs can otherwise undermine collective security and resource values. Norms of reciprocity and restraint are considered the minimum and first step toward informed cooperation. They are fundamental to providing a foundation for informed multilateral consultation.

3.2. Regulating Emerging Technologies

Recent advancements in emerging technologies such as artificial intelligence, robotics, blockchain, quantum

technologies, biotechnology and genetics, and nanotechnologies have raised the question of their implications for international relations. On the one hand, these technologies are subject to increasing research and development in pursuit of a wide range of potential benefits such as social welfare, economic development, and environmental conservation. As examples, AI is claimed to have had significant benefits in areas such as healthcare, communications, and security, while biotechnologies have had profound impacts on stratified and pluralistic societies. At the same time, however, these technologies harbor existential risks and raise the possibility of destabilization of international rules and institutions, with their misuse effectuating threats to state sovereignty, individual rights, and global health and safety¹⁹.

Developing comprehensive regulations is a difficult task – the general pace of technological change often renders implemented regulations outdated. In this setting, regulation emerges on an ad-hoc basis while states grapple with the fast-changing world of blockchain and distributed ledger technology. States are usually assisted in their policy-making by technology creators, researchers, and development personnel from industries and academia. As the policy charter reconstructs the societal and economic impact of technology, industries and academia state that they should, therefore,

be included in policy considerations to ensure that regulation captures all relevant aspects of a technology²⁰. The pace of the ability to develop new agreements and concepts such as AI and ethics demonstrates the inclination of international organizations to adapt international suppliers and requirements in digital governance²¹ and is suddenly retrofitted into a wider domain. But there is also the danger that separation in agreements will be the result of opposition between the major suppliers. To counter such a short-term, fragmented approach, transnational actors and standards will be integrated, and an international consensus will be reached on these critical choice theory concerns. Strategic choices between suppliers and purchasers aim to reduce the risk of transactions. For the digital age, global conformities are concerned with specific norms that take into account the ethical theory of emergent innovations regulation. Technology and ethics are cradled together instead of being dichotomously categorized. Such a stance is common in AI but may lead to abuse²². Measurement of AI pushes its general ideological role—the question of whether it is a friend or a foe, and a sub-focus on deployment through the concept of singularity and weapons. Ethical theory ensures that the leaderless flow of AI is not overlooked in artificial wisdom and limitation, not only in distribution and substitution. It exercises design innovation

in AI, such as algorithmic transparency and ethics, asking the question: who shall do what to whom in algorithmic design? Ethical theory in innovation can prevent the placement of innovation and thus reinforce the study of innovation that does not intrinsically object. Ethical transhumanism can devalue different ethical concerns about the ability of precipitous innovations. It promotes transparency in machines and tackles the question: what is right and wrong?²³ Ethical theory asks the ethics of behavior, just like the advertising of precision in artificial gravity. Since this is only a legitimate problem in operation, the last manual learned ethical theory is seen as the ethics of systems and algorithms by relying on the life-saving car in machine-learning cars. Protecting animals and ensuring ethical effectiveness are the core concerns of this ethical theory AI policy and competition economy face.

4. The Role of Non-State Actors in Digital International Relations

The digital revolution has reshaped the actors and dynamics of international relations. Today, the global stage is inhabited not just by states but also by a variety of non-state entities whose interests, practices, and interactions are actively shaping international and global affairs. In the cyber age, multiple forms of non-state political subjects are actively engaging in digital international relations.

Enhanced by digital technology and connectivity, powerful non-state actors – from non-governmental organizations, transnational corporations, trans-governmental networks, think tanks, activist collectives, to epistemic communities – are seeking to play a more direct role in public and foreign policy debates and decision-making, and they look for opportunities to institutionalize their practices and roles in shaping global policy.²⁴

While many non-state actors aim to prevent, limit, or sanction operations of particular powerful states, some non-state actors have started to build non-cooperative power to challenge or shape state behaviors in digital international affairs. They use diverse strategies to shape policy advocacy and public discourse, such as symbolic protest or identification, technical assessment and criticism, legal and ethical arguments, and pragmatic dialogue. Yet, their strategies greatly differ in accordance with their multifaceted social interests, political values, and policy objectives. Their plural agendas and strategic imperatives have caused legitimacy and representativeness challenges, making many states and civil society networks exercise caution in embracing their intervention in digital policy-making. Besides, the multi-stakeholder model faces inherent tensions between the authorities of sovereign states and international structures and the

interference from non-state actors, who increasingly participate in business functions as well as international politics.

Indeed, non-state actors are showing a strong interest in innovating global internet governance and intellectual property affairs, such as cybersecurity with respect to international terrorism, P2P music file sharing²⁵ networks, or digital intellectual property. There are numerous ways in which states and non-state actors, including non-governmental organizations, renewable energy firms, and outside experts, can collaboratively confront digital policy challenges ranging from climate change to cybersecurity to data governance. Recognizing and acting on these opportunities increasingly is a key role that state and non-state actors are playing. While technological advancements are creating new opportunities for repression, big data digital tracking can also be used to promote societal mental health and environmental awareness through data visualization. Additionally, international relations scholarship that privileges the role of power over narratives neglects non-state actors such as non-governmental organizations, who use narratives to shape policy trajectories and norms in their issue areas²⁶. It is only when these diversely powerful national and transnational actors engage in the societal bricolage of meaning around issues that co-constitutive relationships are fundamentally

structured, meaning that certain relations and interests are limited or enabled between actors in and across discourse communities²⁷. In other words, these actors, like media corporations advancing internet censorship, challenge prevailing state positions on international internet norms and behavior for their issue areas. They also act as a useful moral voice, which is endorsed by a diverse range of countries and internet users who share their issue orientations.

4.1. Tech Companies and Data Governance

Tech companies and data governance internationally, however, a small handful of companies has a near-monopoly on data generation, data processing, and cloud storage and computing. Data governance is more a matter of private corporate governance than a public function of the state. Although these tech giants are obviously shaped by national values, they are also shaped by the competitive logic of the global market. They make their global business models and have a major voice in the global policy debates about data privacy, data security, and data usage. The methods through which these companies develop their policies and strategies reflect quickly changing tides in the international relationships between individuals and society, between technological frontiersmen and conservative regulatory

forces, between the haves and the have-nots²⁸ of technical innovation.

Day to day, the policies and strategies of major tech companies look something like a digital age neocolonialism marked by the constant struggle between colonization, annexation, and moral suasion. The internet is in some sense dictated no more by international laws or norms than it is by chance. Strategy, profit, and unique corporate identity are the driving forces of data governance. As a result, public trust in the largest tech-enabling companies is influenced by these choices in a way that is often oblique: each year's review of technologies demonstrates the more complicated nature of dynamism and adaptive policy among social actors. But the impulse to regulate tech giants according to these complicated dynamics of data policy is often stymied by the challenges of regulating dynamic and relativistic practices. Both researchers and the public are left howling for some stable anchor in the storm of technology. A policy that is flexible, innovative, and robust across applications would be desirable. To be sustainable in the long run, this policy would require more transparency and streamlined accountability across all applications. Such a policy would require both flexibility and stability, adaptation and consistency; it would avoid both the destruction of no regulation and the quagmire of total control. In other words,

it would combine the values of innovation and regulation.²⁹

The tech giants have huge interests in new growth. The largest companies depend on rapidly expanding markets with good scalability for capital and the best distribution channels for new and successful businesses. The smaller companies need cheap and good web hosting that lets them have, store, and serve more dynamic content than ever for ever more specific audiences. The large companies prefer the sacrifices of consolidation across corporations and industries; smaller companies are freer to experiment with relationships to business-to-business, business-to-consumer, and peer-to-peer networks and communications. These large and growing concerns ensure a voice in global data governance: the governance, indeed, ultimately serves them. The governance is stifled by their ability to veto any regulation or law that inconveniences them. Research shows, further, that the business relationship between government and business is often parasitic rather than rich or in any way symmetrical. Especially in the security sector, U.S. cyber forces know much about how to raid and hack – but³¹ only one company has the personal register of every computer's registered owner. In many cases, governments are starved of information that only commercial companies have. Cyber communities often use the technical

knowledge of these commercial companies.

4.2. Civil Society and Online Activism

The Internet and social media platforms have especially enabled and facilitated more individualized and collective online action and mobilization. Using clicks, activists now have the opportunity to equally address individuals while at the same time reaching out to a much larger transnational audience. Grassroots digitally mediated advocacy influencers have become an important source of political legitimacy, making politicians across various sectors pay more attention. The increasing media exposure suggests that global hot topics raise the awareness of all gradations of global citizens.³² It allows for transnational flow through different translocal/local networks of community milieu that are willing to produce and share the same information and common goals in protecting universal rights for local communities. In other words, successful online individual or collective actors can influence thousands of audiences across borders and can move across polities of different sovereign states and still have an effect at different levels.

In the international arena, the flows of communication between local, national, regional, and global levels are the dynamics of global governance, as well as domestic policy that increasingly allow non-state actors to share or shape

normative priorities or, at best, create what is called 'new governance.' This mutual dynamic allows international institutions to become an 'intellectual turnstile' of global and local experts, making use of the legal-institutional and technical foreign aid to manage domestic norm change. The watertight compartmentalization between domestic, international, and transnational is redefined, allowing cross-cutting dynamics of 'democratic advocacy beyond borders' to bridge debates and policies and to advance the transnational synergies of policy or world society. With online social cognitive activism, activists can shape the communication dynamics of pressing public international and cross-border legal issues as they see fit. Together, they create or sustain a particular sense of seriousness in the legal-institutional world to get such humanitarian gestures motivated and ultimately pushed through policies of legal change.³³ Here, we refer to 'new communicative power' that activists have both toward citizens and policymakers to engage, shape, and steer the debates and policies. In sum, individual agents and collective action are not necessarily powerless. Even the most powerless can at least change the dominant discourse in shaping international politics to some extent. The acquisition of new communicative power and repertoires of resistance may add to creative enterprises to explore more equitable and sustainable social change when working in

international or transnational grassroots advocacy studies.

5. Case Studies and Best Practices

The case studies provided in this section offer insights into practical applications of the discussions in the first two sections of the report. From the experience of the Estonian government in cybersecurity to the strategic changes in the communication strategies of intergovernmental organizations, they demonstrate how actors from different contexts are developing strategies and practices to address the security challenges of a digital world. Each presents some of the lessons learned regarding digital transformations of organizations, public services, and/or regional or international engagements. These case studies cover a range of experiences, technologies, and unique solutions. However, despite these differences, some common lessons arise in terms of what the motives and strategies for international digital developments should be³⁴.

These case studies also indicate a few best practices for developing new strategies for foreign, security, and economic policy in a digital age. A main lesson is the need for flexible policy tools. Governments and businesses cannot assume that new communication and information-sharing mechanisms will remain stable over time; established networks and partnerships in digital space will often be reshaped by

technological evolution. Developing digital strategies to face the transformation era was an endeavor characterized by complexity,³⁵ change, and contexts, and it demanded the drafting of guiding concepts that could provide the necessary flexibility and responsiveness. Many best practices involve creating collaborations and partnerships. In line with the concept of 'resilient making,' the practices documented demonstrate a collaborative, team-based approach to digital communication security.

5.1. Estonia: A Digital Society Model

No other country in the world has embraced technology to form a digital society quite like Estonia. With developments such as e-Cabinet, an internet voting system, and a 'data embassy' establishing servers abroad for modern embassies forced to go online, Estonia is a pioneer of e-governance.³⁶ This is at least in part thanks to the high levels of tech engagement, interoperable technology, and trust in both the government and fellow citizens enjoyed within the country. The e-services are extended to and in demand by Estonian residents and Estonians at heart and, as a result, the Estonian public administration has undeniably reaped the benefits in the form of time, money, and manpower. E-governance and the implementation of interconnected e-services between ministries and government agencies have

led to huge boosts in efficiency and transparency and are linked to a corresponding increase in the quality of public services.

Estonia has taken a multi-faceted approach to its digital transformation, developing also a legal and policy framework alongside the necessary infrastructure. For example, the existence of a digital identity system enabled e-residents to access a range of digital services including opening a bank account, declaring taxes, and signing contracts online. The groundwork that went into the early days of Estonian digital infrastructure should also be remembered when attempting to recreate its success elsewhere. Over 35,000 laws were revisited and ‘varying levels of resistance’ were experienced during the dot-com bubble: consolidation efforts were paused because political parties ‘did not want to be seen firing civil servants’³⁷. To maintain infrastructure security and development, study tours, governmental technology consultancy services, and the e-Estonia academy were developed for all interested parties, be they ‘high-ranking’ experts. After all, Ukraine’s first step on the path to a digital society, not an information society, began in 1989 with the turn to technological innovation.

In the digital revolution, e-residents abroad do not need to use representation centers due to their 100% digital engagement with Estonia. Conference

calls and video platforms are similarly only necessary for public administration communication: the government digitized its approach to international relations and then considered opening it up for partnership. Estonia accomplished all of this as part of an extensive program of absolute transparency, sharing every detail of its developments and challenges with any interested party from 2005 onwards³⁸, in order to learn what worked best in terms of providing e-services. Estonia also approached for technological advice, knowing it did not have the requisite expertise, and has continued to collaborate for technological development. This section will be particularly relevant to state governments interested in changing international relations in the digital age.

5.2. The United Nations' Digital Initiatives

For the past two decades, the United Nations (UN) and other international organizations have been looking at how digital capabilities could enhance global interaction and governance. The UN’s digital initiatives were defined by an aim to enhance dialogue between and among member states and relevant stakeholders in different digital formats to enable and expand³⁹ the participation of interested individuals and organizations in global events. In doing so, it aimed at promoting conduct inspired by shared values, which

could improve global cooperation and build, maintain, or provide understanding and empathy to sustain peace.

Most digital initiatives in the UN were motivated by a quest for greater transparency and accountability to ensure good governance of international affairs. They set as a goal the increased participation of affected parties and the commitment to their views and priorities. Some others, though, were more informational and narrative, following the premise that more information passed across all segments of populations could empower global decision-making and impact. However, due to political sensitivities and vested interests in the structures and procedures that have long guided national and international governance, the UN has faced a range of challenges in implementing its digital discourse and data projects. Resistance by member states and insufficient resources have shaped the available measures, but some digital success stories have been identified, featuring novel partnerships between the intergovernmental organization, civil society affiliates, and sometimes key tech organizations⁴⁰. Efforts have also been directed at changing the organization itself in both its structure and culture and aligning itself to the advances brought by the increasingly digital age.

6. Ethical and Legal Considerations in Digital International Relations

Ethical and legal issues emerge in the context of digital international relations. Issues around data privacy, surveillance, and digital rights could affect policy choices and, ultimately, the ways individual rights and state sovereignty are redefined. A need for international cooperation is often evoked, but it is not devoid of ethical implications. Creating an international legal framework in the field of information management, defining a set of security norms and practices for states—these are just a few areas where the issue arises vis-à-vis the foundational principles that international action could be rooted in. Progress in norm development and cyberspace reifies the universality of digital threats, implicating ethical challenges and their role in addressing (or exacerbating) related power dynamics⁴¹.

Data protection and digital privacy become ontologically framed as human rights issues where 'the digital' is concerned. They complement recent conceptual advancements in a global information security policy impacted by hyper-globalization and the implications of 'postmodernity' on communications and world politics. The futility of norms and legal frameworks in potential abridgements of freedom and national security is recognized. Cyberspace is

increasingly becoming an accepted domain of war and a potential threat to global security in the information age. Many international agreements exist on the relations between states in cyberspace. Cybercrime is another major international issue. Ethical issues are also important in the international development of digital technologies. Issues of intellectual property, privacy, and security all have profound ethical implications. As a result, policy and decision-making in digital research development are also fraught with ethical issues. There is a perceived need for an interdisciplinary approach to the study of digital ethics, combining technical expertise with cognitive, behavioral, philosophical, theological, and legal perspectives. Our paper recognizes the importance of these approaches but is concerned primarily with the ethical and, partly, the legal.

6.1. Privacy and Data Protection

Privacy and the protection of personal data have long been the focus of professionals, educators, and activists. Recently, these discussions have gained attention in the general public as well. Individuals are seriously concerned about the use of their information and the potential loss of privacy. It is argued that personal data are essential for those who process them. Indeed, the increasing use of personal data has changed the nature of global trade and the provision of goods and services.

Empowered with idiosyncratic personal data, organizations are able to tailor goods and services to personal desires. However, there has been an enormous cost: privacy and principle.

The protection of the privacy of individuals is a subject of growing importance in the public and political realms. This problem has critical implications for individual freedoms and for the future nature of security within the international system. It seems that the key challenge in the international relations of the Digital Age is to maintain a balance between security and the protection of individuals' rights, including their right to privacy and data protection. This problem will only exacerbate with the proliferation of the internet of things, the changing face of cybercrimes, and the growing interconnections between individuals, the private sector, and public policies worldwide. Of central importance is the role of individuals in defending their own privacy through increased awareness and education, while simultaneously international institutions should play a fundamental role in governing and setting up the normative framework for the governance of global networks and digital trade. Existing instruments and proposals for the governance of digital rights and data protection should be complemented with substantive provisions.⁴²

Recognizing the importance and consequences of privacy and data protection are fundamental steps. The issue for discussion here includes whether the mechanisms that treat privacy as data protection can be installed or are realistic. Privacy and data protection will take a long time to be changed into genuine rights, particularly in an era of shared sovereignty and transnational integration. Privacy and data protection are two distinct notions. The latter is a right in itself and also provides the root for personal rights in the private and public spheres. Privacy means that which is legitimately to be kept unknown or concealed, and the term has been in use since 1822.⁴³ In essence, privacy represents the conscious and voluntary individual decision of this is who I am, and you have no right to know or be involved in the issues of another's life. In contrast, data protection refers to the legislative notions governing the legal obligations from the processing of personal details in data banks. It includes the activities of prevention, repair, and punishment.

6.2. International Law and Cyber Conflicts

While financial, commercial, and political dimensions have definitely reshaped the conditions of international relations, international law is a well-known arena with a different anatomy. Cyber activities, on the other hand, first gained the agenda

of warfare revolution, which is positively shaped by societal developments, and the affected field of international relations is military affairs, specifically national security concerns and expenditures. The story of cyber is very similar to the history of the nuclear era. However, during the time the world passed through the atomic age, international law was not prepared to shape and to be shaped by the consequences of an atomic bomb. In the event of a digital bomb, as a result of the extension of cyberspace from daily life to high politics, the international order becomes secondary in front of the primary society.

International law has already established norms of peacetime prohibitions in the United Nations Charter. These are mostly, respectively, international human rights law and humanitarian law.⁴⁴ The digital content of a cyber activity can transform itself into a research, business, military, or espionage context. The impacts of legally prohibited cyber activity do not stop at the door of the victim state but may disseminate to other states. This has caused some legal scholars to argue that the momentary digital borders have been blurred and that digital territorial integrity is directly affected. The brackets holding the correlation between cyber border crossing activities and territorial sovereignty have begun to dilute in today's digital politics. In addition to the impact of cyber attacks in territorial cyberspace,

another aspect of digital content shall be noted. In the domain of human relations, states shall observe many international norms beginning with non-discrimination. For a victim state, a cyber activity may not be harmful but illegal, and therefore a responsible subject must be held accountable before the international community. In this peace perspective, the right of the state to metadata shall be seen as well as the responsibility of the government of that state, which has the legitimate right to collect data. However, the intrinsic interests of the state parties and the gravity of an act of harming shall be considered to determine whether this act should be seen as a transnational harm. Therefore, the legal criteria are also valid for investigating the proportions of a harmful act in judicial proceedings.⁴⁵

In general, the first step is a decrease in the comprehensive use of technology and weapon sales, while an international agreement among implementer and non-implementer states on the legal level transforms the concept of warfare and establishes a common sense. A common understanding of a cross-border act as a threat shall contribute to this first step, rather than only to a commonly accepted practice and agreement for the concept or backdrop of warfare. In conclusion, territorial sovereignty is not only an important concept but also the cornerstone of the draft of international relations, international law, and warfare itself.

International law is an adaptive and improvisational field, and digital technologies are moving on an exponential path; therefore, both the international governance system and ad hoc agreements on cyberspace are needed.

7. Conclusion and Future Directions

Despite the relatively quick transformation of international relations, this digitalization is still limited. On one hand, there are opportunities as a result of these digital technologies, but there are also challenges and risks. We need to have both a broader outlook and closer insight—a more panoramic and nuanced understanding of the landscape of digitalization and globalization of international relations. We are still in a historical age of transition in which shifts of power influence the possibility of a more effective global governance and global system of cooperation. This is the landscape in which we need to develop and adapt our strategies and international institutional framework for global cooperation. In summary, we can conclude with eight recommendations on global governance and digital technologies in changing international relations. Digital transformation of international relations is not a one-time boom or bust. Instead, it is a historic stage of globalization that will shape and, in turn, will be shaped by the future international order, and is currently encountering many policy, ethical, and

political dilemmas that we have already debated. The governance of the global digital economy is now emerging as a key battleground and a new philosophical underpinning of global politics, and a new geopolitical fault line crossing the globe through institutional multiplicity. Hence, are we just entering a new Cold War, or building a new Concert of powers? The comments made on the issue of digital sovereignty during our summit are interesting but inconclusive. Both lay and

expert reflections on rights and contracts in cyberspace can enfranchise citizens, offering them a sense of control, and/or disempower them because they are internally divisive, leaving citizens more exposed. However, some reflections point to the need to define alternative spaces of digital governance free of the state-corporation dichotomy. We do not conclude here. We invite future studies and action.

4. CONCLUSION

The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article. The conclusion of a research paper needs to summarize the content and purpose of the article.

5. Bibliography List :

¹ G. Sørensen, J Møller, RH Jackson b. Introduction to international relations: theories and approaches 2022 ;P80-99.

² R Kaliisa, B Rienties, AI Mørch, A Kluge -. Social learning analytics in computer-supported collaborative learning environments: A systematic review of empirical studies. sciencedirect.com Cited by 89 Computers and Education Open, 2022 – Elsevier

³ L Zhao, MM Yang, Z Wang, G Michelson - Journal of Business Ethics, 2023 - Springer. Trends in the dynamic evolution of corporate social responsibility and leadership: A literature review and bibliometric analysis. - Journal of Business Ethics, 2023 – Springer p165.

⁴ HP Kaur - Library Progress International,. Traditional Security Threats in a Globalized World: The Changing Dynamics of State-Centered Warfare. Bpasjournals 2024 p122.

⁵ EG KÖSE - ... , Business, Politics, & International Relations ..., The Future of the Modern State: Rethinking the Discourse of “Failed State” with the Emergence of Network (Cyber) State..., 2023 p230.

⁶ Pohle, M Santaniello - Policy & Internet, Wiley Online Library. From

1. **Books** : author’s name (year), full title, publishing, country;

2. **Theses**: researcher, thesis title, college, university, country, year;

3. **Journal article** : author’s name (year), full title of the article, review name, place, volume and number ;

4. **Seminar article**: author’s name (year), full title of the paper, title of seminar, place and date, country ;

5. **Internet websites**: author’s name (year), full title of the file, detailed web site : <http://fulladdress> (consulted on day/month/year).

referance

multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance?. Wiley,2024 p50-55

⁷ P Timmers - Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian ..., - library.oapen.org. Sovereignty in the digital Age. oapen.org2024 p122 .

⁸ Opt ,cit p124

⁹ P Timmers - Hannes Werthner, opt , cit p115 -200

¹⁰ OC Obi, OV Akagha, SO Dawodu, AC Anyanwu... - Computer Science & IT ..., Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Fepbl,p90,2024

¹¹ Ashraf, Y Park, S Hur, SW Kim... - IEEE Transactions ..., A survey on cyber security threats in IoT-enabled maritime industry. yu.ac.kr- ieeeexplore p34,2022

¹² A Aliyu, BE Damilare, AA Hussain, D Omotorsho - researchgate.net. Cybersecurity Measures Safeguarding Digital Assets and Mitigating Risks in an Increasingly Interconnected World. Researchgate,2023,p26-30

- ¹³ M Ghiasi, T Niknam, Z Wang, M Mehrandezh... - Electric Power Systems A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future, Elsevier,2023,p123
- ¹⁴ A Aliyu, BE Damilare, AA Hussain, D Omotorsho,opt,cit p240
- ¹⁵ A Djenna, S Harous, DE Saidouni - Applied Sciences, . Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Mdpj,2021,p90
- ¹⁶ Opt,cit p93
- ¹⁷ W Duo, MC Zhou, A Abusorrah - IEEE/CAA Journal of ...,org. A survey of cyber attacks on cyber physical systems: Recent advances and challenges, ieeexplore.ieee 2021p24-25
- ¹⁸ A Salvi, P Spagnoletti, NS Noori - Computers & Security,. Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. Researchgate,2022 p 70
- ¹⁹ opt,cit 120
- ²⁰ T Zaid, S Garai - Blockchain in Healthcare Today,. Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. nih.gov2024 p 25.
- ²¹ WS Admass, YY Munaye, AA Diro - Cyber Security and Applications,. Cyber security: State of the art, challenges and future directions. sciencedirect.2024p95.
- ²² R Collett - Journal of Cyber Policy, 2021 - Taylor & Francis. Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. Tandfonline2021,p19.
- ²³ N ThiHua, NT Hang, NT Giang, DTN Huy - Ilkogretim Onlinesearch. Human resource for schools of politics and for international relation during globalization and EVFTA. 2022.p191
- ²⁴ Opt,cit p193
- ²⁵ AD Oluwatoyosi - Journal of Information and Knowledge,. Social Media Mobilization and Advocacy: A Case Study,academy2024p69
- ²⁶ Opt,cit p79
- ²⁷ S Huang - VOLUNTAS: International Journal of Voluntary and ..., NGO as sympathy vendor or public advocate? A case study of NGOs' participation in internet fundraising campaigns in China,2023p70
- ²⁸ F Trevisan, M Vaughan, A Vromen -. Story Tech: Power, Storytelling, and Social Change Advocacy,2025p12
- ²⁹ Opt,cit p14
- ³⁰ AD Oluwatoyosi,opt,cit p 71
- ³¹ Opt,cit p76
- ³² T Guerrero-Gómez, A Navarro-Galera... - Sustainability,. Promoting online transparency to help achieve the Sustainable Development Goals: an empirical study of local governments in Latin America,2021p 22
- ³³ Opt,cit p44
- ³⁴ J Virdin, T Vegh, B Ratcliff, E Havice, J Daly, J Stuart - Marine Policy,.Combating illegal fishing through transparency initiatives: Lessons learned from comparative analysis of transparency initiatives in seafood, apparel Sciencedirect,2022p 19
- ³⁵ DR Mishra, D Varshney - Asian Journal of Education and Social ..., fairness, accountability and transparency (FAT) for ethical consumer decision-making: Integrating circular economy principles and digital transformation in global ssrn.2024p8
- ³⁶ Opt,cit pp10_12
- ³⁷ P Quattrone - Accounting, Auditing & Accountability Journal, transparency makes one blind: how to rethink disclosure, account for nature and make corporations sustainable. manchester.2021p74
- ³⁸ Opt,cit p77
- ³⁹ Opt,cit p p79-80
- ⁴⁰ L Pangrazio, J Sefton-Green - Journal of new approaches in educational ..., Digital rights, digital citizenship and digital literacy: What's the difference?. Springer,2021p 242
- ⁴¹ R Geiß, H Lahmann Protection of data in armed conflict. ssrn.2021p 14
- ⁴² C Negri-Ribalta, M Lombard-Platet... - Requirements Engineering, Understanding the GDPR from a requirements engineering perspective—a systematic mapping study on regulatory data protection requirements. springer.2024pp8_13
- ⁴³ C Negri-Ribalta, M Lombard,opt,cit ,p40
- ⁴⁴ G Cifaldi - Soc. & Soc. Work Rev., Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development, HeinOnline2024p130
- ⁴⁵ O Marukhovska-Kartunova, A Bozhkov... - Journal of Lifestyle International Law (SDG'S): Regulation of Conflicts and International Relations. Sdgsreview,2024p20