Vittoria Rose Valerio *33865/410*

The evolution of international diplomacy in the digital age: security, data governance, and artificial intelligence

1. Introduction

The world of diplomacy is experiencing a radical change in the present-day international system due to digital technologies. Unlike in the past where the diplomatic agenda is full of traditional security issues, trade and interstate political relations, in the new times, there are new policy arenas that have thrown the traditional paradigms in international relations. Cybersecurity, privacy, data governance, digital commerce (e-commerce), cybercrime, and artificial intelligence governance (AI governance) are some of these problems, which are increasingly being viewed at multilateral tables of negotiations because of the increasing role of cyberspace and the new technologies in the political, economic, and social life of countries[1].

It is not only the technical aspects of these new areas, but they are also strategic in relevance since they are involved with national security, human rights, economic competitiveness, and supranational legal orders. In the case of cybersecurity, the multilateral discussions have taken cybersecurity as a significant component in establishing the norm of responsible state conduct on cyberspace and averting conflicts caused by cyber-attacks on critical infrastructure[2]. Simultaneously, information security and data control have become foreign policy concerns, since the control of transnational information flows has an impact on the sovereignty of the state in digital space, as well as the basic rights of citizens. These dynamics need to have coherent international agreements that will balance between rights protection, economic development, and collective security[3].

Simultaneously, artificial intelligence is both a threat and an opportunity of modern diplomacy. AI can not only be discussed in the context of negotiation but also serves as an instrument in the process of international policy formulation, analysis, and implementation, forming an overlap of technological governance and international relations. New negotiating priorities based on advanced algorithm management, new ethical concerns, and the geopolitical consequences of technological superiority are shaping new negotiating priorities, both in the multilateral institutional domain and in the process of tech diplomacy[4].

It is in this changing environment that this paper intends to examine how the advent of these new policy issues is reshaping international diplomatic negotiations. We will discuss the challenges and opportunities that the digital diplomacy brings to state and non-state actors through a critical analysis of the literature and the analysis of such cases to understand the significance of the multilateral and multi-stakeholder approach to the challenges of the modern digital world.

---

[1] DiploFoundation. (2025). *Digital diplomacy in 2025: Geopolitics, new topics & tools*. Recuperato da https://www.diplomacy.edu/topics/digital-diplomacy/

[2] Ziani, K. (2025). *Security and reliability in digital diplomacy – review of selected literature*. *Humanities and Social Sciences*, 32(3), 139-152. Recuperato da https://journals.prz.edu.pl/hss/article/download/2064/1537/

[3] DiploFoundation. (2025).

[4] ResearchGate. (2025). *The dual role of artificial intelligence in digital diplomacy and tech diplomacy: Global implications*. Recuperato da https://www.researchgate.net/publication/394309963_THE_DUAL_ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_DIGITAL_DIPLOMACY_AND_TECH_DIPLOMACY_GLOBAL_IMPLICATIONS

2. Theoretical framework: from traditional diplomacy to (cyber/digital) diplomacy

Traditionally, diplomacy has been perceived as an art and practice of international relations, which traditionally was defined as being based on interactions between sovereign states, bilateral and multilateral negotiations and conflict prevention or conflict resolution. The key aims of this classical paradigm were to defend the national security, advance the economic interests, and secure the international stability by using formal and organized means.

The diplomatic practice was dominated by personal relations between diplomats, procedural guidelines and state hegemony. This old structure started changing radically with the rise of the digital technologies and connectivity all over the world. The use of information and communication technologies has pushed the geographical and institutional limits of the diplomacy field even further, leading to so-called digital diplomacy: various practices involving the application of digital technology in foreign policy, as well as the development of new spheres of negotiation in connection with the cyberspace[5]. This notion does not solely apply to communication, but it entails a reconsideration of the means through which states and other international actors make, negotiate, and execute policies in a context where people are becoming more connected[6].

In this more general sense, cyber diplomacy is the phenomenon that is directly related to the governance of cyberspace. It is related to all the diplomatic operations directed at controlling the actions of the states and other participants of the digital environment, and it deals with such issues as cybersecurity, technical cooperation, and prevention of cyber conflicts[7]. In this respect, the cyberspace is not merely the instrument of diplomacy so that it will be a new venue of the international relations. Another aspect of change is the opening of the digital diplomacy to plurality of non-state actors. The involvement in the decision-making and negotiation processes by technology companies, international organizations, technical communities, and civil society has become an enduring phenomenon that contributes to the redefining the nature of global governance. This multi-stakeholder is an international truth where states no longer have an exclusive control over the

[5] DiploFoundation. (2025).
[6] DiploFoundation. n.d. "Technology and Diplomacy." https://www.diplomacy.edu/technology-and-diplomacy/
[7] Christou, George. 2024. *Cyber Diplomacy: From Concept to Practice (Tallinn Paper No. 14)*. https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

regulation of digital infrastructure and the establishment of principles according to which cyberspace should operate[8].

Nevertheless, the fact that traditional diplomacy is shifting into the realm of digital diplomacy does not mean that the old ways of doing things will be fully substituted. Instead, we are seeing a parallel existence and combination of old tools and the emergence of new ways of political and negotiating interaction. Modern diplomacy still has its roots in the past, yet simultaneously embraces the logic, actors, and instruments of the digital ecosystem, with the increased prominence of technology in international relations, particularly in the 21st century.

3. The emergence of new issues in international diplomatic negotiations

The appearance of new policy concerns connected with cyberspace and digital technologies can be regarded as one of the most effective changes in the modern diplomatic agenda. All these problems such as cybersecurity, privacy, data governance, e-commerce, cybercrime, and AI governance do not only demonstrate the increasing centrality of digital infrastructure to contemporary societies, but also bring novel regulatory and geopolitical challenges that need to be addressed by introducing novel and often complex multi-lateral cooperation mechanisms[9]. In that regard, diplomacy is beginning to work in a gray area between security, economics, human rights, and technology.

3.1 International security problem: cybersecurity.

The former area to mention, and probably the most self-evident, is cybersecurity, which has now established itself on the international diplomatic agenda. Energy networks, financial systems, healthcare, telecommunications Cyberattacks on critical infrastructure are today being counted as threats to national and international security. To address these dangers, the United Nations has created several negotiating forums, such as the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), which is expected to formulate principles and norms that states must follow in cyberspace[10]. Such negotiation procedures have brought some major breakthroughs such as establishing applicability of international law in cyberspace and encouraging confidence-building activities. Nevertheless, the states still differ in terms of the character of the rules, the extent of their

[8] Affari Internazionali. 2022. "Diplomazia, genere e diversità nel cyberspazio." https://www.affarinternazionali.it/diplomazia-genere-e-diversita-nel-cyberspazio/
[9] Christou, George. 2024.
[10] United Nations. (2021). *Open-Ended Working Group on Developments in the Field of ICTs.* https://www.un.org/disarmament/ict-security/

bindings, and the establishment of liability concerning cyberattacks, and cybersecurity is one of the most delicate points on the geopolitical agenda[11].

3.2 Data protection and privacy as international relations matters.

Meanwhile, the matters of privacy and the security of personal data have become the important issues of diplomacy. The introduction of the General Data Protection Regulation (GDPR) in the European Union has served to redefine the standards of data protection in the whole world that not only impacted the national laws but also international frameworks on information transfer across the borders[12]. Privacy in this case is a strategic aspect not merely in the safeguarding of basic rights, but also economical and geopolitical intercourse. It is in a tenuous balance of security, technological innovation and data protection where diplomatic talks are becoming more and more concerned with the necessity to balance these three elements.

3.3 Cross-border data flows and data governance.

Data governance is a collection of regulations and procedures that entail the way data is gathered, handled, shared, and utilized. Cross-border data flows have become a center stage in the operation of digital economies and global value chains in the international setting. Nonetheless, the methodologies of the states on the subject of digital sovereignty, localization of data, and ownership of digital infrastructure by the state or individuals are too different[13]. These differences manifest themselves in the multilateral forums, in which the various regulatory models of open, regulated, and heavily statist are discussed, which makes data governance a field of strategic rivalry, yet also a subject of diplomatic collaboration.

3.4 E-commerce and digital trade

Other places where the digital technology has joined the international negotiations are e-commerce. The World Trade Organization (WTO) has initiated digital trade negotiations over the last few years, focusing on the taxation of online services and consumer protection, algorithms transparency, and

---

[11] Christou, G. (2024)
[12] European Commission. (2018). *General Data Protection Regulation (GDPR)*. https://commission.europa.eu/law/law-topic/data-protection_en
[13] UNCTAD. (2021). *Digital Economy Report*. https://unctad.org/publication/digital-economy-report-2021

free movement of business-related data[14]. These discussions indicate that the digital aspect cannot be detached anymore to the conventional international trade, but it is a natural progression of one.

3.5 Internet crime and international judicial cooperation

The topic of cybercrime relates to the joint action to address the transnational cybercrimes, including fraud, ransomware, illicit trafficking, and massive information system breaches. The primary tool in this area is the Budapest Convention on cybercrime, the initial international treaty on the issue, which facilitates cooperation between states in courts[15]. Concurrently, the UN is developing a new international convention on cybercrime, and its goal is to further expand collaboration to even more countries, regardless of the large disparities in politics and laws among the countries that are signatories.

3.6 The new frontier of AI governance in diplomacy.

Lastly, one of the latest issues that are on the diplomatic agenda is artificial intelligence governance. The OECD and UNESCO have worked out ethical, transparent, and responsible principles and suggestions to encourage the ethical, transparent, and responsible development of AI systems[16]. The aspects of accountability, algorithm bias, security, work effects and military application are some of the issues that are being discussed internationally. AI governance is thus a new area where states are competing to be regarded as leaders in technology yet simultaneously collaborate to prevent the risks to the system, and safeguard the rights as the basis.

4. New actors and new negotiating dynamics

The advent of the digital concern on the diplomatic agenda has introduced a radical shift in not only the content of the international negotiations, but also their participants and the manner in which they are being held. Historically, traditionally states-dominated diplomacy that is mediated through formal institutional mechanisms has been gradually opening up to a plurality of actors and processes that are

---

[14] World Trade Organization (WTO). (2024). *E-commerce and Digital Trade.* https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

[15] Council of Europe. (2024). *Budapest Convention on Cybercrime.* https://www.coe.int/en/web/cybercrime

[16] OECD. (2019). *OECD Principles on Artificial Intelligence.* https://oecd.ai/en/ai-principles

indicative of the complexity of cyberspace and global infrastructures of the digital world[17]. Here, dynamics of negotiation have turned out to be more fluid, multi-level, and technically advanced.

4.1 Multi-stakeholder diplomacy and plurality of actors

The increasing centralization of the multi-stakeholder model, which involves states, international organizations, technology corporations, the technical community and civil society as important participants in decision-making and consultation spaces, is one of the most powerful developments. Such a strategy is noticeable especially in the process of governing the Internet and the discourse of global digital policies, as seen in the case of the Internet Governance Forum (IGF), which, among others, was created by the United Nations as an avenue to engage in all-inclusive discussion of the topic of cybersecurity, digital rights, and data governance[18]. The inclusion of non-governmental actors specifically large platforms and international technology firms depict the reality that much of the strategic digital infrastructure is being privately owned and operated. This provides businesses with a sort of diplomatic status of deciding to establish security, privacy and data management standards, making international negotiations more hybrid and cross-sectoral[19].

4.2 Technicality, professionalism and capability imbalances

A second important factor issues the high degree of technicality that is involved in digital negotiations. The definition of standards on cybersecurity, AI governance, or data governance needs an interdisciplinary knowledge base that constitutes a combination of computer science, law, economics, and political science. The phenomenon, in turn, has required the need of more coordination between ministries, security agencies, data protection authorities, and technical standardization bodies[20]. This complexity however also creates capacity imbalances among states. Largely, countries that possess a higher level of technological resources and systems of administration have a negotiating edge and many developing countries may find it difficult to be completely involved in the international decision-making mechanisms on matters of digital concern. This is why it is why

---

[17] Bjola, C., & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. https://global.oup.com/academic/product/digital-diplomacy-9780415749031

[18] United Nations. (2023). *Internet Governance Forum (IGF)*. https://www.intgovforum.org

[19] Christou, G. (2024)

[20] OECD. (2019). *OECD Principles on Artificial Intelligence*. https://oecd.ai/en/ai-principles

many multilateral agenda are increasingly emphasizing the notion of capacity-building in order to enhance the inclusive engagement in the global digital policies[21].

4.3 Security, rights and development intersection

The other unique dynamic relates to the cross-cutting nature of digital issues. The problems of negotiation cannot be limited to one sphere: security, economy, or human rights, but he/she needs a combination. As an illustration, the definition of the cybersecurity standards also has a concurrent impact on the safeguarding of the basic rights and the economic competitiveness, along with the political stability[22]. The result of this increased interdependence has been the restructuring of the internal governance mechanisms in most states to establish coordination functions on digital policies and to deepen cooperation between the ministries. Simultaneously, when it comes to regulatory differences between various governance paradigms (that include Europe, the US, and China) the conflicts are likely to manifest in the global arena, which causes fragmentation but also the slow process of establishing international standards[23].

Overall, it can be concluded that diplomatic negotiations in the digital age have become marked with a sophisticated web of actors and interests, where the capacity to converse between worlds that are traditionally deemed separate, politics, technology, industry, and civil society, is becoming a prerequisite of constructing effective and legitimate international regimes.

5. Brief case studies

It is practical to examine some of the iconic cases to obtain a tangible perspective of how the emerging digital challenges are transforming the international diplomatic agenda. The most relevant among them are the discussions on cybersecurity by the United Nations and multilateral efforts on the regulation of artificial intelligence.

5.1. Cybersecurity and the regulations of the actions of states of the cyberspace

The first major case is the gradual elaboration of international regulations on cybersecurity at the United Nations. Since the beginning of the 2000 decade, the General Assembly has created various Groups of Governmental Experts (GGE) with the mandate of analyzing the impacts of cybersecurity

---

[21] UNCTAD. (2021). *Digital Economy Report.*
https://unctad.org/publication/digital-economy-report-2021
[22] Christou, G. (2024)
[23] UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence.*
https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

on peace and stability in the international system. In 2013 and 2015, this work has published significant reports that understand the applicability of international law to cyberspace and the necessity of establishing measures of cooperation and transparency between states to do so[24].

The process is backed by the Open-Ended Working Group (OEWG) since 2019 and, unlike the GGE, is accessible to any of the member states. This move indicates a change toward more inclusive types of negotiation, in accordance with the increased significance of cyberspace across the globe and the necessity to make the political basis of agreements stronger[25].

Nevertheless, the disparity between the states is still not negligible, especially in terms of the extent to which cyber-attacks should be regulated and what should be considered as the state responsibility. Nevertheless, the case of the UN evidence that cybersecurity is becoming one of the key diplomatic concerns and digital negotiation is contributing to the creation of new models of international regulating the world[26].

5.2 AI governance of international organizations.

The second scenario is the Artificial Intelligence Governance. Since the end of the 2010s, several international organizations have initiated projects to establish moral standards and rules on how to use AI responsibly. OECD has been one of the first institutions to establish a multilateral regulatory framework, having adopted the Principles on Artificial Intelligence in 2019 that espouse principles of transparency, accountability, and respect of human rights[27].

In 2021, the UNESCO implemented the Recommendation on the Ethics of Artificial Intelligence, which was accepted by its member states as the first international regulatory tool on AI. The document highlights the necessity to make sure that the development of intelligent technologies occurs in a human-centered way and proposes specific steps to be undertaken by states, which include ethical impact assessment and enhanced public governance[28].

---

[24] United Nations. (2015). *Group of Governmental Experts on Developments in the Field of ICTs in the Context of International Security (A/70/174)*.
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf
[25] United Nations. (2021). *Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security*.
https://www.un.org/disarmament/ict-security/
[26] Christou, G. (2024).
[27] OECD. (2019). *OECD Principles on Artificial Intelligence*.
https://oecd.ai/en/ai-principles
[28] UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.
https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

These processes demonstrate that modern diplomacy is not restricted to consider military or commercial matters anymore, but rather it is engaged in the establishment of ethical and regulatory standards to the new technologies that radically impact societies and the world economy. Simultaneously, the pluralism of negotiating forums; OECD, UNESCO, G20, United Nations indicate a danger of institutional fragmentation, yet also the dynamism with which the international community is attempting to react to the difficulties presented by AI.

These two cases demonstrate that cybersecurity and AI governance are extremely strategic fields of diplomacy, in which security, rights, economics, and technological power are overlapping. They further affirm that digital diplomacy does not represent a peripheral sector, but it is part and parcel of modern global governance.

6. Open challenges and prospects

Open problems and perspectives Digital issues are introduced into the international diplomatic agenda, which poses many unresolved problems, not only in the definition of common regulatory frameworks but also in the operation of the multilateral system. The first acute problem is that of institutional fragmentation. Problems of cyberspace are now spread across an array of forums and organizations diverse in their competencies, approaches, and legitimacy, such as the United Nations, the OECD, UNESCO and the WTO, to the multi-stakeholder platforms of the IGF[29]. This plurality can promote regulatory innovativeness, yet it simultaneously implies that it may generate overlaps, regulatory conflicts, and regime rivalry, and the standardization of regulations is more challenging to sustain globally[30].

The second challenge is that of values and governance models. Specifically, clashing sides are more individual rights-based and data protection-based approaches (European model) and more information control or market and innovation priorities-oriented approaches[31].These contrasts are mirrored in global negotiations, which create geopolitical divisions which may impede the establishment of cooperation regimes in sectors like cybersecurity and AI governance. Concurrently, the field of digital diplomacy is emerging as a competitive field in terms of technological and regulatory dominance.

---

[29] United Nations. (2023). *Internet Governance Forum (IGF).* https://www.intgovforum.org

[30] Christou, 2024

[31] UNCTAD. (2021). *Digital Economy Report.* https://unctad.org/publication/digital-economy-report-2021

Capacity asymmetry among nations is also another important issue. Those nations that possess more technology and institutional capability can negotiate more or at least derail the agenda and the negotiation outcomes whereas most of the developing countries are likely to be sidelined by the world decision making process. This is why the international cooperation is gradually incorporating the capacity building and technical assistance programs, where it is intended to advance more inclusive and sustainable digital governance[32].

This is another area of concern, the systemic security of cyberspace. Increasing the interdependence of digital infrastructures with the growing number of emerging technologies such as artificial intelligence introduces new vulnerabilities that can increase the risk of conflict, political interference, disinformation, and human rights violations[33]. That is why it is high time to establish norms and mechanisms of mutual trust that would help to minimize the risks of escalation and digital incidents and, at the same time, not to eliminate technological innovation.

Although there are these challenges, there are also several opportunities in the future. The increasing international attention to digital concerns is enhancing the convergence of common values, including the necessity to develop ethical and transparent technological growth that would not infringe the basic rights. Meanwhile, the complementation of the multi-stakeholder models and communication between the state and business communities provide new opportunities of collaboration and diplomatic creativity[34].

7. Conclusions

The rise of such problems as cybersecurity, privacy, data governance, e-commerce, cybercrime, and AI governance has dramatically changed modern diplomacy, broadening its scope and agenda. Even in a setting characterized by regulatory fragmentation and geopolitical competition, digital diplomacy today needs interdisciplinary competencies, new participants, and more permeable manifestations of multilateral collaboration. These developments become the chance to create more transparent and rights-oriented global regimes despite the challenges. Digital diplomacy is thus not an ancillary area, but instead, a structural feature of the 21st-century international governance.

---

[32] UNCTAD. (2021).
[33] OECD. (2019). *OECD Principles on Artificial Intelligence.* https://oecd.ai/en/ai-principles
[34] United Nations. (2023). *Internet Governance Forum (IGF).* https://www.intgovforum.org

Bibliography

Affari Internazionali. 2022. “Diplomazia, genere e diversità nel cyberspazio.” https://www.affarinternazionali.it/diplomazia-genere-e-diversita-nel-cyberspazio/

Christou, George. 2024. *Cyber Diplomacy: From Concept to Practice (Tallinn Paper No. 14).* https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

Council of Europe. 2024. “Budapest Convention on Cybercrime.” https://www.coe.int/en/web/cybercrime

Cyber Diplomacy Toolbox. n.d. “Cyber Diplomacy.” https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

DiploFoundation. n.d. “Technology and Diplomacy.” https://www.diplomacy.edu/technology-and-diplomacy/

DiploFoundation. 2025. *Digital Diplomacy in 2025: Geopolitics, New Topics & Tools.* https://www.diplomacy.edu/topics/digital-diplomacy/

European Commission. 2018. “General Data Protection Regulation (GDPR).” https://commission.europa.eu/law/law-topic/data-protection_en

OECD. 2019. *OECD Principles on Artificial Intelligence.* https://oecd.ai/en/ai-principles

UNCTAD. 2021. *Digital Economy Report.* https://unctad.org/publication/digital-economy-report-2021

UNESCO. 2021. *Recommendation on the Ethics of Artificial Intelligence.* https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

United Nations. 2015. *Group of Governmental Experts on Developments in the Field of ICTs in the Context of International Security (A/70/174).* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf

United Nations. 2021. *Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security.* https://www.un.org/disarmament/ict-security/

United Nations. 2023. “Internet Governance Forum (IGF).” https://www.intgovforum.org

World Trade Organization. 2024. “E-commerce and Digital Trade.” https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm