idn brief

June 2024

Cyberdiplomacy

DIRETORA
Isabel Ferreira Nunes
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
António Baranita e Luísa Nunes
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional

ISSN 2182-5327
Depósito Legal 340906/12

idn Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017 Lisboa
Telf: +351 211 544 700
idn.publicacoes@defesa.pt

Cyberdiplomacy

The Importance of Cyber Diplomacy in International Relations Today

Rui Tavares Lanceiro
Assistant Professor at Faculdade de Direito da Universidade de Lisboa.

Cyber diplomacy has emerged as a crucial aspect of international relations in the digital age. This article explores the evolution of cyber diplomacy, key theoretical frameworks, notable case studies, and the challenges and opportunities it presents. It concludes by highlighting the significance of cyber diplomacy in promoting global security and stability, with a particular emphasis on international law.

Introduction

Cyber diplomacy is a term classically used to refer to the use of diplomatic strategies and negotiations to address issues related to cyberspace, including cybersecurity, internet governance, and digital rights. As the digital landscape continues to expand, the significance of cyber diplomacy has grown, strongly impacting international relations. This article examines the evolution of cyber diplomacy, its theoretical framework, with a particular focus on international law, and the challenges and opportunities it presents.

The Evolution of Cyber Diplomacy

The concept of cyber diplomacy has its roots in the late 20th century, coinciding with the rise of the internet and the increasing interconnectedness of global communications. Early efforts focused on establishing a regulatory framework for internet governance, with organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) – which is not a classical international organization – playing pivotal roles. The early 2000s saw significant developments, such as the establishment of the United Nations (UN) Group of Governmental Experts (GGE) to discuss the threats posed by the use of information and communication technologies, possible cooperation, and other issues of international information security. Since 2004, several GGE have continued to work on these topics and issued reports with conclusions and recommendations that have been well-received by the General Assembly of the United Nations and welcomed by UN Member States

In recent years, cyber diplomacy has evolved to address a broader range of issues, including cybersecurity threats, cybercrime, and the protection of critical infrastructure. Major international actors, such as the United States, the European Union, and China, have developed sophisticated cyber diplomacy strategies to protect their national interests and promote global stability.

The Theoretical Framework of Cyber Diplomacy

The field of cyber diplomacy extends traditional diplomatic practices to address issues such as cybersecurity, cyber threats, cybercrime, and the militarization of cyberspace. *Cybersecurity* refers to the measures taken to protect computer systems, networks, and data from cyber-attacks. Cyber threats encompass a wide range of malicious activities, including hacking, data breaches, and

cyber espionage. *Digital diplomacy* involves the use of digital technologies and platforms to conduct diplomatic activities and engage with international audiences. Today, cyber diplomacy should be considered an equal and essential part of a broader and holistic state cybersecurity policy toolbox.

Theoretical approaches to cyber diplomacy include realism, liberalism, and constructivism. Realism emphasizes the importance of state sovereignty and the competitive nature of international relations, highlighting the need for robust national cybersecurity measures. Liberalism focuses on international cooperation and the creation of global norms and institutions to address cyber threats. Constructivism examines the role of ideas, beliefs, and social structures in shaping state behaviour in cyberspace.

Over time, there is also a growing consensus that International Law plays a critical role in shaping the norms and principles that govern state behaviour in cyberspace. For example, Article 2(4) of the UN Charter, that prohibits the use of force against the territorial integrity or political independence of any state, is relevant to cyber operations that could be construed as acts of aggression. In the same way, International Humanitarian Law, particularly the Geneva Conventions, is considered applicable to cyber operations in the context of armed conflict, ensuring the protection of civilians and the proportionality of attacks.

International Law also provides specific answers to the challenges presented in this field. For instance, the Budapest Convention on Cybercrime is the first international treaty on crimes committed via the internet and other computer networks, seeking to harmonize national laws, improve investigative techniques, and increase cooperation among nations. In this area, there have been discussions at the UN level for drafting a legally binding international treaty to counter cybercrime. However, five years after the beginning of the negotiations, they are still ongoing, with parties unable to reach an acceptable consensus, with countries unable to agree on wording that would balance human rights safeguards with security concerns.

Another example is the Tallinn Manual on the International Law Applicable to Cyber Warfare, which was developed by international legal experts, and provides a comprehensive non-binding analysis of how existing International Law, especially *jus ad bellum* and International Humanitarian Law, applies to cyber operations and cyber warfare.

Another significant case is the establishment of the Paris Call for Trust and Security in Cyberspace, a multi-stakeholder initiative launched by France in 2018. The Paris Call aims to promote principles for secure and stable cyberspace, garnering support from governments, international organizations, and private sector entities. This initiative highlights the role of cyber diplomacy in building consensus and fostering international cooperation.

Challenges and Opportunities in Cyber Diplomacy

Cyber diplomacy faces several challenges, including the difficulty of attributing cyber-attacks to specific actors, the tension between state sovereignty and the global nature of cyberspace, and the varying levels of cybersecurity capabilities among nations. These challenges complicate efforts to develop and enforce international norms and agreements.

Attribution of cyber-attacks remains one of the most significant challenges in cyber diplomacy. The anonymity afforded by cyberspace allows state and non-state actors to carry out attacks without immediate detection or accountability. This creates difficulties in holding agents responsible and in formulating appropriate responses.

State sovereignty is another complex issue. The global nature of cyberspace transcends national borders, leading to jurisdictional ambiguities and conflicts. Countries must navigate the delicate balance between asserting their sovereign rights and cooperating on international norms that govern cyberspace.

Despite these challenges, cyber diplomacy also presents significant opportunities. Public-private partnerships can enhance cybersecurity by leveraging the expertise and resources of the private sector. These partnerships are essential as many critical infrastructures, such as financial systems and telecommunications networks, are owned and operated by private entities. Collaborative efforts can lead to the development of advanced cybersecurity measures and the sharing of vital threat intelligence.

International treaties and agreements can establish common standards and norms for state behaviour in cyberspace. The creation of such frameworks can foster a more predictable and stable cyber environment.

Capacity-building initiatives can help developing countries improve their cybersecurity infrastructure and resilience. By providing technical assistance, training, and resources, these initiatives can elevate the overall global cybersecurity posture, making it harder for cyber threats to exploit weaker links in the international system.

Emerging technologies, such as artificial intelligence and quantum computing, will further shape the future of cyber diplomacy. These technologies offer new tools for enhancing cybersecurity but also present new risks and challenges that require coordinated international responses. For example, AI can be used to detect and respond to cyber threats

more swiftly, while quantum computing could potentially break current encryption standards, necessitating the development of new cryptographic techniques.

References

Aldrich, R. J., & Karatzogianni, A. Cyber Power and Cyber Diplomacy, in George Christou, Wilhelm Vosse, Joe Burton and Joachim Koops, *Handbook on Cyber Diplomacy*, Palgrave MacMillan, (forthcoming, 2025).

Barrinha, A., & Renard, T., 2020. Power and Diplomacy in the Post-Liberal Cyberspace. *International Affairs*, 96(3), 749-766.

Choucri, N., & Goldsmith, D., 2012. Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, 68(2), 70-77.

Christou, G., 2024. Cyber Diplomacy: From Concept to Practice. *Tallinn Paper,* No. 14. NATO Cooperative Cyber Defence Centre of Excellence.

Council on Foreign Relations (CFR). (2018). *Cyber Operations Tracker.* Council on Foreign Relations.

European Union Agency for Cybersecurity (ENISA), 2020. *ENISA Threat Landscape 2020.* European Union Agency for Cybersecurity.

Feakin, T., & Weaver, J., 2020. Cyber diplomacy, in Eneken Tikk and Mika Kerttunen, eds., *Routledge Handbook of International Cybersecurity.* Abingdon: Routledge, 277-285.

Kello, L., 2017. *The Virtual Weapon and International Order.* Yale University Press.

Klimburg, A., 2017. *The Darkening Web: The War for Cyberspace*. New York: Penguin Press.

Langenhove, L. V., & Boers, E., 2021. Multilevel Diplomacy in Europe in the Digital Century, in George Christou and Jacob Hasselbach, eds., *Global Networks and European Actors: Navigating and Managing Complexity.* Abingdon, Oxon and NY: Routledge.

Maurer, T., 2018. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

Meyer, P., 2012. Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda. *The RUSI Journal,* February/March, 157(1), 14-19.

Nye, J. S., 2017. Deterrence and Dissuasion in *Cyberspace. International* Security, 41(3), 44-71.

Painter, C., 2018. Diplomacy in Cyberspace. *American Foreign Service Association*, June. Available at https://afsa.org/diplomacy-cyberspace

Riordan, S., 2019. Cyberdiplomacy: Managing Security and Governance Online. Cambridge: Polity Press.

Singer, P. W., & Friedman, A., 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

United Nations Group of Governmental Experts (UNGGE), 2015. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations.

Cyber-diplomacy: A Field in Flux

André Barrinha

University of Bath

Three decades ago, cyber-diplomacy did not exist. The interest in Information and Communication Technology (ICT) as a vector of change in international relations was limited to a few mostly technical organisations, and a restricted number of states.

The late 1990s saw a growing interest on the topic, but we would have to wait almost a decade before states started to fully grasp the challenges and opportunities brought by the formation of this new policy domain.

As often happens in situations where issues acquire a strategic importance, diplomats started to be deployed to the frontline of emerging discussions around the international governance of cyberspace. In the last 15 years, governments around the world have created offices, bureaus, or appointed experts and diplomats to engage with peers, non-state actors in regional and international organisations to discuss and agree on norms of responsible state behaviour, capacity building or confidence-building measures in cyberspace. This has led to what I label as the diplomatisation of cyber policy, in which many of the structures, practices and institutions of diplomacy progressively helped shape this global governance domain.

The emergency of cyber diplomacy can be seen as an example of the general process of how states adjust to new policy domains. In this particular case, there have been a myriad of external dynamics that contributed to it, including the international institutionalisation of the field through formal and informal fora (such as the UN Group of Governmental Experts and the Open Ended Working Group on the role of ICTs in international security), but also internally, where specific political agents (as in the US, Australia or the UK) or large-scale cyber-attacks (as in the Netherlands) pushed individual states to be more pro-active in this domain.

State responses were often more dependent on their respective national diplomatic cultures than on the idiosyncratic nature of the issue.

Institutional answers tended to be more in line with what was done in-house regarding similar domains, than in other states. The result is a varied set of diplomats and actors with a wide-range of functions, roles, and levels of responsibility and importance. This is where we start to notice the unsettled and transient nature of cyber diplomacy.

From over 50 interviews we conducted with officials, diplomats and experts, it became clear that there was no consensus on what cyber diplomacy is, or on what being a cyber diplomat entails. For some, it is a narrow field encompassing issues of interstate International cybersecurity, for others it is a wider field that includes issues such as internet governance or even digital economy. In some cases, being a cyber diplomat was limited to following discussions within the UN; for others it included responsibilities regarding disinformation, 5G and even Artificial Intelligence. Some of these responsibilities came with the role (as in the US, where in 2022 Nathaniel C. Fick was appointed Ambassador at Large for Cyberspace and Digital Policy), some were added after the role was created (such as in Australia, Brazil, and Portugal). Given the omnipresence and fast development of digital technology, it is only natural that diplomatic responsibilities in this domain evolve.

In 2017, Denmark created its Techplomacy, and appointed its first Tech Ambassador with offices in Beijing, Copenhagen and Silicon Valley to interact with a broad range of state and non-state actors, including directly with Big Tech companies. Since then, other states have joined in. In 2020, the European Union, who already had a Cyber Diplomacy office within its European External Action Service, created a separate one for Digital Diplomacy to deal with a broad range of tech-related issues, from supply-chains to content moderation.

For now, cyber diplomacy seems to sit in parallel with these other developments, but it is likely that given the multiple overlaps, they may merge in the near future and cyber diplomacy could then become a branch of tech (or digital) diplomacy. Whereas we could see this as the result of state bureaucracies trying to swiftly respond to new challenges, it also leaves open the possibility that underneath its centenary status, diplomacy is a practice in constant flux, in which its rituals and institutions serve to hide the fragilities and inconsistencies of what often are underplanned solutions. In short, through the diplomatisation of cyber policy we can see both the strength of statecraft - in shaping how and where issues are discussed - but also diplomacy's fragile and transient nature. In that regard, cyber diplomacy may not be more than a reflection of a broader, often hidden reality.

Text originally published on the *Hague Journal of Diplomacy blog*

How Important is the Cyberdiplomacy to the Deterrence in Cyberspace?

Helder Fialho Jesus

Navy Captain

Cyberdiplomacy is a critical component for handling the complexities of the digital world. It encompasses the application of traditional diplomatic principles such as negotiation, cooperation, and conflict resolution to address cybersecurity, digital governance, internet freedom, and other aspects of the digital domain. As the digital realm continues to expand its influence on global affairs, economy, and society, cyberdiplomacy becomes increasingly essential in managing the volatility, uncertainty, complexity, and ambiguity (VUCA) of our world.

Deterrence in cyberspace is a key aspect of cyberdiplomacy. It involves using various measures and strategies to dissuade potential adversaries from engaging in hostile or malicious cyber activities. Drawing from traditional deterrence theory, the goal is to convince adversaries that the costs or consequences of their actions outweigh any potential benefits, thereby preventing them from taking harmful actions in cyberspace.

Cyberdiplomacy plays a crucial role in deterrence in cyberspace for several reasons. Firstly, it involves the development of norms, treaties, agreements, and other diplomatic instruments to promote stability, security, and cooperation in cyberspace. Joseph Nye explained in his paper "Deterrence and Dissuasion in Cyberspace" that norms serve as a deterrent mechanism in cyberspace. By establishing norms of responsible behavior, cyberdiplomacy can adjust the behavior of state and non-state actors in cyberspace, contributing to deterrence efforts. The first serious discussion of the matter occurred in the late 1990s. In 1998, the General Assembly passed Resolution 53/70, a Russian initiative that invited States to share their views on information security and the "advisability of developing international legal regimes to provide security of global information and telecommunications systems and to combat terrorism and criminality". Efforts in cyberdiplomacy within the United Nations, through initiatives like the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), have been instrumental in fostering global consensus and advancing the development of norms for cyberspace governance. These groups operate independently but complementarily, contributing to the

overall goal of enhancing cybersecurity and stability under the auspices of the United Nations.

Effective cyberdiplomacy efforts can exert normative pressure on state and non-state actors to adhere to established rules and norms of behavior in cyberspace. By reinforcing international consensus on responsible state behavior and condemning violations, diplomatic initiatives can shape perceptions of acceptable conduct and deterrence strategies in cyberspace. An example can be the effort by Western countries to kill the Russian tech industry due to the invasion of Ukraine in February 2022 as a retaliatory action of punishment.

Moreover, cyberdiplomacy within the UN contributes to conflict prevention and peacebuilding efforts by addressing cybersecurity challenges that have the potential to escalate into conflicts or undermine international peace and security. UN-led cyberdiplomacy initiatives can reduce tensions and mitigate the risk of cyber-related conflicts by promoting dialogue, cooperation, and confidence-building measures among states. By establishing clear rules of engagement (ROE) and channels for communication, cyberdiplomacy can help build trust among nations and reduce the likelihood of misunderstandings or escalations in cyberspace, ultimately contributing to conflict prevention and peacekeeping efforts.

Additionally, cyberdiplomacy initiatives often involve the development and implementation of confidence-building measures (CBMs) aimed at enhancing transparency, communication, and trust among states. These measures contribute to confidence-building and reduce the perception of insecurity, thereby deterring aggressive behavior in cyberspace. An example are the 16 CBMs within the OSCE's toolbox to reduce the risks of inter-state conflict in cyberspace, which can be used by states to share their national views on cyber threats, strategy and legislative documents on cyber/ICT security, or ways to categorize events that affect key infrastructures.

Diplomatic efforts are also essential for addressing challenges related to attribution and accountability in cyberspace. Through diplomatic discussions and negotiations, countries can work together to develop mechanisms for accurately attributing cyberattacks and holding responsible actors accountable. The prospect of diplomatic consequences can serve as a deterrent to state-sponsored cyber activities. Although attributing cyberattacks is challenging due to technological, legal, and political reasons, it is essential for holding responsible parties accountable for harmful actions and maintaining peace online. The EU sanctions system, stemming from the 2017 Cyber Diplomacy Toolbox, is a commendable method for promoting accountability in cyberspace and a deterrence tool.

Furthermore, cyberdiplomacy enables countries in their alliances and coalitions to address shared cybersecurity challenges collectively. Through diplomatic channels, states can coordinate responses to cyber threats, share best practices, and leverage collective capabilities to enhance deterrence posture in cyberspace. A good example is the decision of the European Council against two people and one organization that were involved in or accountable for the cyberattack that targeted the German Federal Parliament (*Bundestag*) in April and May of 2015. The information system of the parliament was the target of the cyberattack, with a substantial quantity of information stolen, compromising many email accounts, including the previous German Chancellor Angela Merkel, which left the system inoperable for several days.

Cyberspace has an increasingly noticeable impact on societies and International Relations, leading to organizational adaptations, which in the case of the diplomatic world takes place with the emergence of new ambassadorial positions, with designations linked to cyberspace (USA), cybersecurity (UK), technological (Denmark), digital (France), cyberdiplomacy (Portugal) or related to hybrid threats (Spain), among others. And these ambassadors naturally have an important role when it comes to deterrence in cyberspace, within the framework of their countries' alliances.

In conclusion, it is paradoxical that the country that took the lead in proposing standards for cyberspace is also linked to judgments for violating codes of conduct and international norms. Cyberdiplomacy constitutes an element that can contribute to deterrence in cyberspace despite the difficulty of measuring its performance as a preventive measure. As the digital landscape continues to evolve, effective cyberdiplomacy will remain central in addressing emerging threats and maintaining stability and security in cyberspace.

Capacity Building for EU Cyber Diplomacy: A Fundamental Element

João Assis Barbas

Adviser at Instituto da Defesa Nacional

The purpose of this paper is to give visibility to EU Capacity Building in the cyber domain, as an essential element of the EU Cyber Diplomacy approach, in line with the United Nations (UN) Charter[1], the EU principles and values[2]. The UN Group of Governmental Experts (GGE) on Developments in the Field of

Information and Telecommunications in the Context of International Security[3], proposed several recommendations in four reports[4] in cyber-related domains, such as Capacity-building, to enhance information security in the international community.

Capacity-building involves measures that are essential to strengthen global efforts on securing Information and Communication Technologies (ICTs) and their use, particularly in developing countries.

The UNGGE's main recommendations regarding capacity building in developing countries stress bilateral, regional, multilateral, and international efforts to secure ICT use and infrastructures, strengthen national legal frameworks, combat criminal and terrorist use of ICTs, and identify and disseminate best practices; establish incident response capabilities; promoting the use of education, training, and awareness-raising programs to help overcome the digital divide; encourage analysis and study on matters related to ICT security; cooperation initiatives to improve mutual assistance; assistance to improve the security of critical ICT infrastructure, develop technical skills, appropriate legislation, strategies, and regulatory frameworks.

The 2021 Report from the Open-End Working Group[5] (OEWG) emphasizes the importance of cooperation, transparency, information sharing, and capacity-building efforts to promote a secure and stable ICT environment at the national, regional, and international levels. The report also urges states and other stakeholders to provide financial or technical support for capacity-building initiatives. Capacity-building is also underlined as essential for developing countries concerning ICTs within international security, mitigating vulnerabilities, and reinforcing resilience and security measures.

At the European Union (EU) and aligned with the UNGGE recommendations from three of the four approved reports[4], the 2016 EU Global Strategy[6] emphasized the importance of cooperation with third parties in the cyber domain as a key aspect of the European Union's foreign and security policy and stressed the "State and Societal Resilience" of countries in EU surrounding regions.

The 2020 EU's Cybersecurity Strategy[7] addresses also key aspects related to capacity building with the EU's surrounding areas, such as supporting the development of legislation and policies in line with EU cyber diplomacy policies and standards; and assistance to address malicious cyber activities.

The 2022 EU Strategic Compass[8] recognizes the interconnected nature of cyber threats and the need for collaborative efforts to address them effectively. It emphasizes the importance of cyber cooperation and enhancing cyber resilience and capabilities not only within the EU but also in its neighbouring regions, as a key aspect of its security and defence strategy.

The EU aims to protect, detect, defend, and deter cyberattacks through various policies and initiatives. EU's Cyber Cooperation Strategy is supported by collaboration with partners and capacity building. For the EU, collaboration is crucial in countering hybrid threats, foreign information manipulation, and interference. Supporting partners in enhancing cyber resilience and deploying experts in case of cyber crises are fundamental elements of capacity building.

Overall, the Strategic Compass underscores the importance of cyber cooperation and capacity building with EU surrounding areas as part of a comprehensive approach to enhancing cybersecurity and addressing cyber threats collaboratively and inclusively.

Meanwhile, the EU cyber legal framework incorporated three other relevant documents that encompass capacity-building aspects. While the Regulation (EU) 2019/881 – Cyber Security Act[9] – primarily focuses on enhancing cybersecurity within the European Union, some provisions indirectly address cooperation and capacity-building with EU surrounding regions in the context of cybersecurity, through ENISA. That could potentially have positive effects by promoting best practices, information sharing, and collaboration in neighbouring regions.

The Cyber Resilience Act[10] also highlights the importance of cooperation and capacity building with surrounding regions in the context of cybersecurity, via bilateral Mutual Recognition Agreements for "conformity assessment and marking of regulated products"; the promotion of a global cyber resilience environment to strengthen the cybersecurity framework within and outside the EU. Furthermore, it addresses the cross-border nature of cybersecurity threats and the risks faced by Member States for the same products with digital elements.

In line with this extensive framework, the EU Cyber Solidarity Act[11] proposed by the European Commission endorses strengthening the readiness of critical entities[12] across the EU and enhancing solidarity by establishing common response capacities against "significant or large-scale cybersecurity incidents", by providing support to cyber-incidents for third countries associated with the Digital Europe Programme[13].

Alongside the normative framework, the European Union has been promoting cyber capacity building in its surrounding regions through various initiatives and programs, such as extending the benefits of the EU Digital Single Market

to the Eastern Partnership through the EU4Digital Initiative; enhancing cybersecurity and cyber resilience in Eastern Partnership (EaP) and third countries via Cybersecurity East the EU Cyber Capacity Building (EU CCB) Program; Supporting the improvement of cybersecurity frameworks and capabilities in the Western Balkan countries; Providing short-term technical assistance to neighbouring countries to help them align with EU standards and practices through Technical Assistance and Information Exchange (TAIEX)[14].

In summary, the European Union outlined a mature charter, initiatives, and programs to promote cyber capacity-building in its surrounding regions through various initiatives and programs that are in line with UN GGE and OEWG recommendations and that will contribute to the security and defence of European societies and partners in surrounding regions.

References

[1] https://www.un.org/en/about-us/un-charter

[2] https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en

[3] https://disarmament.unoda.org/ict-security/

[4] 2010, 2013, 2015, and 2021.

[5] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[6] European Union (2016). Global Strategy. Shared Vision, Common Action: A Stronger Europe Shared Vision, Common Action : A Stronger Europe. In *EEAS*, https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

[7] European Parliament, & Council of the European Union (2020). The EU's Cybersecurity Strategy for the Digital Decade. Join(2020) 18 Final, 18 Final. https://ec.europa.eu/newsroom/dae/redirection/document/72164

[8] Council of the EU (2022). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[9] https://eur-lex.europa.eu/eli/reg/2019/881/oj

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

[12] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

[13] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[14] https://eur-lex.europa.eu/EN/legal-content/glossary/taiex-technical-assistance-and-information-exchange.html