

Cyber-Diplomacy in the Digital Era

Piergiorgio Valente | IAFEI Overall Technical Committee Chair President CFE Tax Advisers
Europe Chair GTAP Global Tax Advisers Platform

In the digital age, cyber-diplomacy has become an essential tool for international relations, addressing the challenges posed by cyberspace. Cyberspace can sometimes seem very abstract and incomprehensible. But in 2024 cyberspace is considered the fifth domain of warfare. Alongside the more traditional sea, land, air and space, cyberspace has become a space with active collaboration but also a target for attacks. As in our relations on the "real world" we need diplomacy to keep the peace, we also need secure, commonly understood cyber-diplomacy, to keep war away from our cyber-space.

Cyber-diplomacy involves the use of diplomatic strategies to manage issues such as cybersecurity, digital trade, and internet governance. While traditionally focused on national security, cyber-diplomacy now overlaps significantly with legal and economic considerations. Cyber-diplomacy is the term used to describe the diplomacy in cyberspace (the use of diplomatic resources and the diplomatic functions to secure national interests and peace in cyberspace).

Despite ongoing efforts through public awareness campaigns, research and development, and educational initiatives, individuals and organizations remain today still highly vulnerable to cyber-attacks. As the world becomes more and more connected, the impact of cyber-attacks extends beyond individuals and can affect critical infrastructure, government systems, and international networks, posing significant global challenges.

The future of cyber-diplomacy will depend on nations' ability to negotiate a shared vision for a secure, open, and digital world with a great potential. It is widely recognized in today's world that the ability to shape the rules in cyberspace can grant significant influence over other stakeholders. However, perspectives on what is considered right or wrong might vary significantly across regions. For instance, views on privacy differ significantly between countries, and so do opinions on different surveillance practices. As a result, we are witnessing a new form of competition, reminding us of the space-race during the Cold War, with different regions striving to set standards for cyberspace regulation.

Frameworks that Help to Shape Cyber-Diplomacy

The rise of so-called data localization laws has further complicated the economic landscape of cyber-diplomacy. These laws require data to be stored within a country's borders in order to protect national security and privacy. But on the other hand, these laws can also act as barriers to international trade. Negotiations in cyber-diplomacy often focus on balancing these concerns, seeking to harmonize regulations and facilitate the free flow of data while safeguarding privacy. For example, agreements like the EU-U.S. Data Privacy Framework aim to resolve conflicts between differing privacy standards and enable smoother cross-border data exchanges [European Commission. "Questions & Answers: EU-US Data Privacy Framework." European Commission, 9 July 2023].

EU-USA Data Privacy Framework ensures that the USA ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities can transfer personal data to participating U.S. companies without the need for additional data protection measures. This framework provides EU individuals, whose data would be transferred to participating companies in the US, with several new rights [European Commission. "Questions & Answers: EU-US Data Privacy Framework." European Commission, 9 July 2023].

The global digital economy also demands cyber-norms and standards of behavior for states in cyberspace. Because even as it seems abstract and something that we cannot see or touch, we all participate actively in that “abstract” space. By establishing agreements on what can be considered as acceptable cyber activities, nations can reduce the risk of economic disruptions and foster trust among their international partners. These are just some examples of diplomatic efforts that are crucial for building a secure environment for digital trade and investment.

European Union Member States have acknowledged the urge to set down common rules in a series of actions already for a while. Revised guidelines together with a common toolbox against cyber-attacks have been created by the Council of the EU [Council of the European Union. “Revised Implementing Guidelines, Cyber Diplomacy Toolbox.” 2023].

Although, conceptually, cyber-defense was initially meant for the protection of military assets, its influence is widening, given that the military sphere, just like the civilian sphere, depends on a safe cyber-space to protect critical infrastructure such as electric grids, water systems, banking, transport, communication systems and the flow of goods and services. The same attitude is shared by various States around the world, taking unilateral or multilateral positions regarding cyber-attacks and cyber-diplomacy.

In recent years, a variety of proposals have emerged concerning frameworks and regulations aimed at governing cyberspace. Notable examples include the EU Cybersecurity Strategy, the Cyber Diplomacy Toolbox, the General Data Protection Regulation (GDPR), the Convention on Cybercrime (commonly referred to as the Budapest Convention), and the OECD Cybersecurity Policy Framework. These initiatives highlight the active efforts of different players to shape the landscape of cybersecurity. Despite great progress, the world still lacks a unified and commonly accepted global framework for cybersecurity. There are many proposals and projects, but one certain set of rules, with what all the stakeholders agree, is still missing.

Legal Challenges of Cyber-Diplomacy

Digitalization of our everyday life, together with activities and relationships with the state one lives in, and economic relations is a norm in today’s world. The aim of overall digitalization is to simplify the way of doing things, to save time and to make everything more efficient. However, by simplifying one thing, we might unintentionally complicate something else. The inevitable digitalization brings with it also many new forms of crime and wrongdoings that need to be penalized and legally dealt with. This raises some issues.

One of the primary legal issues in cyber-diplomacy is the application of international law to cyberspace. For instance, the issue of recognition - determining who is behind an occurred cyber-attack - or even what exactly is a cyber-attack - is particularly problematic. There are some rules set on this topic, but the task remains still complicated. Cyber operations can be conducted anonymously, making it difficult to identify the offenders and apply legal consequences, such as, for example, the Budapest Convention on Cybercrime, that has established guidelines for cooperation and harmonization of national laws. Moreover, not all nations have adopted these agreements, and significant players like Russia or China have decided to use alternative frameworks, challenging the establishment of a universal legal approach to cyber threats [“CETS 185 - Convention on Cybercrime]. Their main point of concern being the question of sovereignty.

The question of state sovereignty in cyberspace remains highly controversial not only for China and Russia. While some countries stand for sovereignty over their use of digital space, others emphasize the importance of an open and connected internet and cyber-space. Missing a cohesive legal framework

stays on the way of effective diplomatic efforts and increases the risk of conflicts escalating into cyber warfare.

Cyber-Diplomacy and Digital Economy

Cyber-diplomacy also plays a critical role in shaping the digital economy, now more than ever. Cybersecurity is considered as a top priority for global economic stability as huge part of businesses operate online. Recently, key economic sectors such as commerce, transport, finance and energy have become more and more reliant on digital technologies, and the risk from cyber threats and attacks keeps on growing.

Recent data highlights the substantial growth of the digital economy, significantly outpacing traditional so-called brick-and-mortar sectors in recent years. For example, in the United States, the value added by the digital economy increased by 6.3% in 2022, while the overall economy grew by only 1.9% [The Journal of the U.S. Bureau of Economic Analysis. "U.S. Digital Economy: New and Revised Estimates, 2017-2022", 6 December 2023]. Over the last decade, there has been a clear pattern of rapid growth in the digital sector compared to traditional industries. It emphasizes the growing importance of digital services such as e-commerce, cloud computing, and telecommunications, which have become key drivers of economic activity ["OECD Digital Economy Outlook 2024 (Volume 1) : Embracing the Technology Frontier | OECD Digital Economy Outlook." OECD iLibrary, 2024].

It is the case not only in the USA. Globally, the digital economy's expansion has been remarkable as well. The OECD reported that digitalization has contributed significantly to GDP growth across its member countries. The rise of e-commerce and digital services has transformed industries, particularly after the COVID-19 pandemic, which strongly pushed digitalization and innovation ["OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier | OECD Digital Economy Outlook." OECD iLibrary, 2024].

As from one hand, globalization and overall connectivity of the world's economy is positive and enriching by creating economic growth and trade possibilities, on the other hand it makes the whole economy also very vulnerable. Cyber-attacks, such as intellectual property theft, system run downs by hackers and tax-crimes pose significant threats to businesses and can even disrupt global supply chains. Therefore, it is of utmost importance that cyber-diplomacy in collaboration with cyber-security is applied when operating in digital economy in order to prevent crimes from happening.

Tackling Tax Crime in The Digitalized Economy

With the overall digitalization of our lives, tax and other financial crimes are more global than ever which can undermine the rule of law as well as public confidence in the legal and financial system. As mentioned previously, technological development brings with it endless positive opportunities, but unfortunately it creates also new risks and ideas for crimes. The growth of cybercrimes, including the increasing misuse of cryptocurrencies and people who can create opaque structures and move around money increasingly in real-time, has been noteworthy. All these developments give fighting tax crimes a new importance. This new era calls for increasing international co-operation and for all jurisdictions to have a robust domestic set of legal and operational tools in place to effectively detect, disrupt and sanction tax crime offenders and those who enable tax crimes [OECD. "Fighting Tax Crime – The Ten Global Principles, Second Edition." 2021]. What is more, uncertainty in the taxation of online business models can have adverse implications for tax compliance.

OECD published a report in 2021 outlining The Ten Global Principles, which detail the comprehensive set of tools that countries should aim to implement to tackle the new problems of tax crimes. These include implying tougher laws to criminalize tax offenses, developing a unified tax crime strategy to

detect threats and target criminal activities and establishing mechanisms to seize the criminal gains following a conviction [OECD. "Fighting Tax Crime – The Ten Global Principles, Second Edition." 2021].

Furthermore, the report proposes that jurisdictions dedicated to helping developing countries' tax capacity-building efforts, such as the Addis Tax Initiative or the G7 Bari Declaration, should investigate more effective collaboration with developing countries. This collaboration should concentrate on improving tax crime investigations and encourage more widespread adherence of the Ten Principles. Proposals for next steps include sending expert trainers to the OECD International Academy for Tax and Financial Crime Investigation, participating in the Tax Inspectors Without Borders pilot program for criminal investigations, assisting with the implementation of the Tax Crime Investigation Model, and collaborating on regional or bilateral projects [OECD. "Fighting Tax Crime – The Ten Global Principles, Second Edition." 2021].

The OECD's Task Force on Tax Crimes and Other Crimes (TFTC) will continue to support international coordination in the fight against tax crime, particularly in areas where coordinated global action is critical, such as asset recovery and dealing with professional facilitators. Furthermore, the TFTC should collaborate with other stakeholders to develop a coordinated strategy for addressing cross-border tax crimes. This strategy should include mechanisms for risk identification, potentially expanding available data sources, and ensuring effective data and information-sharing agreements. All of this must be adapted to the digital world, using cyber-diplomacy to prevent threats and cyber-security to tackle potential criminals.

Conclusion

Cyberspace contains an enormous amount of economic, social, and political possibilities. If properly managed, it can foster long-term growth and shared success for all. However, without proper regulation, it risks becoming a battleground for destructive confrontations. Cooperation through diplomacy among states, international bodies, and supranational authorities is essential to harness its benefits while mitigating the risks.

While the digital economy and technical advancements provide limitless benefits, they also expose governments and businesses to cyberattacks and vulnerabilities. To create a secure and thriving cyberspace, it is critical to develop widely accepted norms that apply to all participants. Furthermore, the rising digital economy presents difficult challenges such as taxation and financial crime. Cybercrime, cryptocurrency misuse, and sophisticated money laundering networks emphasize the need for close monitoring and international collaboration. Addressing these risks will require continuous innovation, coordinated efforts and shared responsibility to secure the future of the digital age.

Diplomacy has been a cornerstone for international relations, and overall relations between people, since the beginning of time. Cyber-diplomacy will be the next cornerstone of our future world, shaping how nations collaborate, resolve conflicts, and protect our shared digital space. As technology continues to be the protagonist of global connectivity, the ability to navigate and negotiate in cyber space is essential for ensuring peace, security, and continuous development. Embracing cyber-diplomacy is not just a necessity, it is an investment to ensure a stable and cooperative digital future.

Professor Piergiorgio Valente is the Managing Partner of Crowe Valente. He is a known International Tax Advisor who has held various leadership roles in European and global Tax Organizations like President of the CFE Tax Advisers Europe and Chair of the GTAP Global Tax Advisers since 2019 and President of International Tax-Policy Commission at CNDEC. He is active in the Academia and is the Professor of Diritto Internazionale and International Tax Law at the Link Campus University in Rome.

