

TECH DIPLOMACY 2.0: EXAMINING THE INTERSECTIONS BETWEEN INDUSTRY AND GOVERNMENTS IN INTERNATIONAL RELATIONS

Clara COTRONEO^{1,2}, Raluca CSERNATONI^{3,4}

¹ Institute of Security and Global Affairs, Faculty of Governance and Global Affairs,
University of Leiden, The Netherlands
c.cotroneo@fgga.leidenuniv.nl

² Global Governance Institute, Brussels, Belgium
c.cotroneo@globalgovernance.eu

³ Carnegie Europe, Brussels, Belgium

⁴ Centre for Security, Diplomacy and Strategy (CSDS),
Vrije Universiteit Brussel (VUB) Brussels, Belgium
Raluca.Csernatoni@vub.be

Abstract: In 2017, the government of Denmark appointed the world's first tech diplomat to represent its interests before tech companies in Silicon Valley. Since then, various states and international organisations, including the United Nations (UN) and the European Union (EU), have followed suit. This has led to a rapid increase in the number of tech diplomats appointed worldwide. Despite the number of tech diplomats having grown rapidly in the past 8 years, the concept and practice of 'tech diplomacy' remain relatively unexplored in academic and professional circles alike. Through the practitioners' insights and the analysis of empirical vignettes drawing from the EU, this paper explores the practice of tech diplomacy by identifying its key characteristics, players, processes, and objectives. The aim of this paper is to trace the contours of this emerging practice, contribute to scholarly understandings of how diplomacy is evolving during the so-called Fourth Industrial Revolution, and assess the broader impact of technological developments on international relations and global governance.

Keywords: tech diplomacy, international relations, corporations.

TECH DIPLOMACY: A SHORT INTRODUCTION

In 2018, DiPLO, a not-for-profit organisation dedicated to the study and improvement of diplomacy, published a report mapping the interactions between governments and tech companies in Silicon Valley (Horejsova et al., 2018; Rauchbauer & Ittelson, 2018). At the time it was published, the report was considered pioneering in that it shed light on a diplomatic function and practice that was still emerging. However, only five years later, a new, updated report concluded that the practice of 'tech diplomacy' had developed fast, becoming more structured on both policy and administrative levels (Ittelson & Rauchbauer, 2023). This new report, based on the analysis of the interactions between 37 tech diplomats and their counterparts in tech companies, showed dynamic and diverse exchanges. Despite this internal evolution, however, the practice of 'tech diplomacy' remains largely overlooked in both academic and practitioners' circles.

Yet, from an international relations perspective, this apparent neglect obscures how tech diplomacy both draws on and stretches core theoretical frameworks. For instance, rather than fitting neatly into the traditional state-centric diplomacy of classical realism, tech diplomacy

exemplifies what Keohane & Nye (1973) had already termed as complex power and interdependence, where multiple channels (state and nonstate), a mix of issue areas, and the declining utility of coercion create a more networked and layered field of interaction. It also reflects a polycentric and hybrid foreign policy environment in which authority and influence are distributed across states, corporations, international organisations, and transnational epistemic communities, requiring what some scholars now describe as ‘orchestration’ of governance, where public actors convene, align, and steer private and third-sector actors without full hierarchical control (Renda et al., 2024). Tech giants, under certain enabling conditions of capability reach, and institutional embeddedness function as geopolitical actors in their own right, shaping norms, strategic alignments, and even crisis management, not merely as objects of diplomacy but as interlocutors and agenda-setters (Aiken et al., 2025). This renders tech diplomacy simultaneously a practice of engagement, co-constitutive norm formation, and bargaining among asymmetric but interdependent actors. Consequently, the blurring of the traditional boundaries between public and private diplomacy further means that legitimacy, trust-building, and narrative framing become central tools, as observed in the evolving EU and Silicon Valley interfaces, where nonstate actors are treated as essential partners rather than externalities (Bjola & Kornprobst, 2024). The emerging literature thus frames tech diplomacy not as a marginal adaptation but as a transformative modality of international relations, one that institutionalises the multi-stakeholder dialogue, leverages the regulatory power as the de facto soft infrastructure, and seeks to stabilise contested digital orders amid great-power technological rivalry and normative contestation, especially in the case of emerging and disruptive technologies like AI (Csernaton, 2025).

Against this backdrop, the objective of this paper is to provide an overview of the studies conducted so far on tech diplomacy and identify the key features, key players, processes and outcomes. Focusing on the European Union’s (EU) tech diplomacy envoy and the organisation’s development in this area will support this preliminary investigation and help further scholarly and policy understandings of the practice. The next section offers an overview of the main discussions surrounding the conceptualisation and use of the phrase ‘tech diplomacy’. Next, the actors, tools and scope of this diplomatic practice are explored by drawing on case studies from international organisations, such as the United Nations and intergovernmental organisations, such as the EU. The latter’s approach to tech diplomacy is the object of the following section of the paper, which concludes with a summary of the points discussed and key recommendations for future research and practices.

STATE OF THE ART

While the references to ‘tech diplomacy’ have multiplied in scholarly and grey literature, the meaning of this phrase remains unclear. That is, what the practice entails and how distinct it is from other forms of diplomacy are yet to be defined. A conceptual review of how the terms ‘cyber’, ‘digital’ and ‘tech’ are used in reference to different diplomatic practices has identified key differences in their policy areas and objectives (Mesquita & Brito, 2024). According to Barrinha & Renard (2017), ‘cyber diplomacy’ refers to diplomatic practices focusing on cybersecurity and governance in the cyberspace, from international law and security perspectives. Instead, ‘digital diplomacy’ has been used in reference to diplomatic practices that make use of social media tools for public diplomacy (Bjola & Kornprobst,

2025). According to this categorisation, digital diplomacy is different from cyber and tech diplomacy because the use of the Internet and information and communication technologies (ICTs) is a means, rather than an object of diplomatic practices.¹ Finally, 'tech diplomacy' shares with the other two categories of diplomacy core features, including means, focus areas and objectives (Mesquita & Brito, 2024). However, 'tech diplomacy' refers to a dynamic diplomatic practice, which focuses primarily on digital innovation and emerging technologies and entails a systematic engagement with Big Techs and other non-state actors (Bjola & Kornprobst, 2025).

Though there is no single agreed definition for 'tech diplomacy' in either scholarly or practitioners' works, this paper considers tech diplomacy as a category of diplomatic practices that is uniquely identified because of its principal interlocutors: foreign affairs governmental officers on the one side, and representatives from tech companies, and companies from various sectors involved in the development of the digital, emerging and disruptive technologies, on the other. In this sense, this paper aligns with Mesquita and Brito's view that tech diplomacy designates 'policies conducted by foreign affairs personnel to approach the innovation centres that are developing game-changing technologies' (Mesquita & Brito, 2024, p. 25). With regards to the purpose of tech diplomacy, this paper aligns with the view put forward by the world's first tech diplomat who claimed that the objective of tech diplomacy is to address technology and digitalisation as a foreign policy field. Tech diplomacy, therefore, refers to diplomats' engagement with their counterparts in private companies working on the development of digital, emerging and disruptive platforms, services and technologies. Tech diplomats deal with cross-sectorial policies, including in innovation, regulatory issues, digitalisation, cyber-security, digital inclusion, trade, amongst others. As such, the work of tech diplomats shares similarities and partly overlaps with that of cyber and digital diplomats. Based on the interviews carried out with representatives from MFAs, the same foreign affairs office can wear different hats, switching between the function of 'cyber' diplomat to that of 'tech' diplomat, for example. Cyber, digital and tech diplomats all engage with non-governmental actors on issues related to the societal, economic, and security impacts of the digital, emerging and disruptive technologies, platforms and services. However, the most prominent and distinguishing feature of tech diplomacy resides in the recognition of the tech industry players as significant actors in international relations. Tech diplomacy, therefore, represents a new, additional practice in foreign diplomacy that can be uniquely identified precisely because it engages with 'a new someone to whom governments must speak', namely tech companies (Mesquita & Brito, 2024, p. 31).

Recent analyses of the role of tech companies in international relations (Broeders & Taylor, 2017), security (Cotroneo & Leonard, 2025) and economy (Abels, 2024) have led scholars to re-evaluating the relationships between states and companies. Some have argued that tech companies and states are inter-dependent (Abels, 2024; Cotroneo & Derbyshire, forthcoming) and that transnational corporations are international actors (Broeders & Taylor, 2017). According to Broeders et al. (2025), multinational corporations hold corporate agency due to the rise of informality in international relations and governance and to their infrastructural

¹ For others, 'digital' diplomacy focuses on digital policies broadly, whereas, 'e-diplomacy' or 'virtual diplomacy' refer to diplomatic practices using ICTs

power. As Abels (2024) and Broeders et al. (2025) have shown, multinational corporations own infrastructures that are critical to states and societies. In the case of tech companies, they hold both infrastructure power in the form of data centres, for example, and capabilities for enhancing states' competitiveness and security (Cotroneo & Derbyshire, forthcoming; Cotroneo & Leonard, 2025). Scholars like Garcia (2022) argue that tech diplomacy signals a change in the understanding and practice of diplomacy, once conceived as state-centred, entailing primarily inter-state negotiations. From Garcia's perspective, the traditional international relations frameworks, characterised by state-centric views have become inadequate for understanding diplomacy in the age of the Fourth Industrial Revolution. According to Garcia, tech diplomacy is born of states' efforts to adapt their (diplomatic) strategies to the new technological developments and the pervasive adoption of the emerging and disruptive technologies at the individual and societal levels. With technology re-shaping world politics, economies and social interactions, tech corporations have become significant interlocutors for governmental officials. From Garcia's perspective, tech diplomacy is a new, rather than an additional form of diplomacy, born from a radical re-thinking, from a state perspective, of how negotiations should be conducted and with whom.

Another reason why tech diplomacy may be symptomatic of a radical shift in international relations is because of the increasingly crucial role of technology as an instrument of national identity, sovereignty, security and competitiveness (Csernaton, 2022). As an instrument of soft power, technological innovation and high-tech prowess are part of the inter-state global competition. That is, states build narrative rhetorics showcasing technological innovation and maturity levels to boost their stature and strengthen their influence on the international stage. Examples are incorporations of the emerging technologies, such as artificial intelligence (AI), quantum computing and biotechnology into official communications to imply that a nation is future-oriented and equipped to face global challenges. Moreover, innovation success can be used to showcase a vibrant, competitive ecosystem for the industry and competitiveness nationally and globally. Finally, the services provided by some tech companies, such as social media platforms, are increasingly used as instruments for manipulating narratives, to the detriment of the competing states' reputations and even national stability (Bradshaw & Howard, 2018). This leads tech diplomats to engage in conversations that are cross-cutting, addressing the implications that AI and other emerging and disruptive technologies have for state sovereignty, security, democratic functioning, as well as for data privacy (Csernaton, 2024b).

In this respect, it could be argued that Big Tech's latest developments in generative AI models are reshaping international relations by inserting powerful nonstate actors into the heart of the global power dynamics and forcing a re-conceptualisation of tech diplomacy. Platforms and AI systems, owned by a few dominant firms, wield near-monopoly influence over information flows, enabling targeted political messaging and algorithmic amplification that blur the line between citizens and consumers and give the corporate actors outsized leverage over the democratic discourse. This concentration of technical capacity means states no longer negotiate solely with other states; they must engage, regulate, and sometimes constrain private AI gatekeepers as part of their diplomatic strategy (Csernaton, 2024a). At the same time, AI lowers the barrier for foreign interference, producing synthetic content and deepfakes that can be weaponised across borders to destabilise elections and public

trust, intensifying the geopolitical competition in the information domain. Thus, an effective tech diplomacy requires multilateral governance frameworks, harmonised standards, transparency mandates, and accountability mechanisms that bridge the state and corporate responsibilities, while building coalitions to resist the digital authoritarian diffusion and protect democratic resilience.

Other examples include the involvement of both the defence industry and increasingly the Big Tech in developing autonomous weapon systems that use AI, which showcases the work of the tech sector in the development of emerging and disrupting technologies with military purposes (Cotroneo & Derbyshire, forthcoming). Indeed, Big Tech and the defence industry have become intertwined pillars of contemporary tech diplomacy, especially in emerging and disruptive domains like military AI. As Csernatoni (2024c) argues, corporate tech firms are now key actors in a ‘trillion-dollar arms race’ over foundational AI models, blurring the traditional state-centric boundaries of security innovation. Their dual-use technologies, initially developed for civilian purposes, are increasingly repurposed for defence, creating ‘mission creep’ and forcing diplomats to engage simultaneously with sovereign states and powerful nonstate providers. This convergence elevates tech diplomacy into a multilayered negotiation space where norms, access to critical components, for instance, advanced semiconductors, and ethical guardrails become strategic leverage points. The defence industry, in partnership with Big Tech, accelerates such capability development while amplifying the geopolitical competition, making governance coordination urgent: states must align with firms on standards like meaningful human control, transparency, and risk mitigation to prevent their destabilising proliferation. The EU, leveraging its normative weight and regulatory tools, is well-positioned as a potential broker of multistakeholder coalitions to tame runaway military AI and integrate corporate actors into a shared framework of responsible development. Effective tech diplomacy thus requires reconciling corporate sovereignty with collective security governance.

This paper assumes that, because of these developments, some states have recently adapted their foreign policy priorities, diplomatic practices and models to address tech companies as new relevant players in international affairs. One of such adaptive practices has been the establishment of dedicated positions within states’ diplomatic ranks to discuss issues concerning digital, emerging and disruptive innovations directly with the tech industry. States’ decision to engage directly with the tech industry, therefore, is seen as an adaptive strategy, following from states’ recognition of multinational tech companies as significant interlocutors, due to their control of critical infrastructures and of almost every layer of the technological stack, as well as their role in driving technological trends and innovation, markets and economic development, inter-state competition, including in international security. This new practice also signals the (perceived) interdependence between tech and state actors, which interact with one another and their environment to advance their objectives.

Overall, it could be argued that tech diplomacy should be seen as both a bilateral outreach and as a relational and constitutive practice in which states, institutions, and firms co-create the architectures, norms, and strategic imaginaries that govern the emerging socio-technical systems. Private tech actors are not passive recipients of foreign policy but active corporate diplomats with their own external strategies, embedded interests, and capacities to shape global agendas. For instance, an engagement can become a form of mutual ‘regulatory

diplomacy' where rulemaking over critical technological domains is negotiated, contested, and sometimes co-authored across public-private boundaries. This relationality leads to an asymmetric interdependence: tech firms possess knowledge, platforms, big budgets, computing power, excellent human capital, data, and infrastructure that confer both material power and epistemic authority, while states and institutions retain normative legitimacy and coercive backing, creating layered bargaining spaces where legitimacy, trust, and framing are as crucial as the material concessions.

Furthermore, tech diplomacy operates through the logic of hedging, where states aim to align and guide corporate behaviour indirectly, leveraging standards, codes of practice, and partnership incentives, rather than through command-and-control, effectively governing from a distance. These dynamics produce hybrid public-private governance regimes, where the global digital order results from iterative translations between sectoral tech priorities, geopolitical competition, including digital sovereignty concerns, strategic autonomy, and economic security, and shared problem-solving, such as AI safety or supply chain resilience. Ultimately, the performative narratives embedded in these engagements, for instance, about 'trusted AI', 'secure digital sovereignty', or 'responsible innovation', shape expectations and lock-in trajectories, demonstrating that tech diplomacy is as much about making futures credible (Csernaton, 2024b) as it is about managing the present risks.

ACTORS, TOOLS AND SCOPE: SKETCHING THE CONTOURS OF TECH DIPLOMACY AS A PRACTICE

To move from these high-level dynamics to institutional practice, states and international organisations have created dedicated human and organisational nodes, such as tech diplomats, who serve as boundary spanners, knowledge brokers, and managers in the hybrid governance space described previously. These envoys translate the abstract logics of hedging, normative diffusion, and performative future-making into concrete engagement strategies: they embed themselves in industry ecosystems, most visibly in Silicon Valley, align corporate incentives with public goals through dialogue and soft coordination, and help stabilise the competing sociotechnical imaginaries (Csernaton & Martins, 2023) about disrupted technological futures by mediating between regulatory expectations and technological capacities. In doing so, tech diplomats do not simply represent their governments. It could be argued that they perform the active work of the networked statecraft, linking standard-setting, geopolitical positioning, including digital sovereignty and strategic autonomy concerns, and shared problem-solving across public-private divides. Their appointments thus materialise the desired governance architectures that make the technological and digital futures legible, actionable, and socially stabilised.

Indeed, tech diplomats are appointed by individual states or groups of states, such as international organisations like the UN or the EU. These two influential organisations have recently created tech diplomacy positions and strategies to ensure that progress, research and development in innovative digital, emerging and disruptive technologies are in line with their interests and values. Recent appointments include that of Amandeep Singh Gill, appointed by the United Nations Secretary-General as Envoy on Technology and Gerard de Graff, appointed as EU Senior Envoy for Digital to the United States (U.S.) in 2022 and now representing the EU in Silicon Valley. These two appointments show that international organisations are

constituting diplomatic offices specifically to address foreign policies that centre around the digital, emerging and disruptive technologies. Because the principal interlocutors for the tech diplomats are the tech industry representatives, whose primary deployment location is a new centre of global power, namely Silicon Valley.

Beyond this descriptive analysis, recent scholarship has complicated the understanding of tech diplomacy's instrumental repertoire by situating it within the broader structural and normative dynamics of the global digital order. In this respect, tech diplomacy is not simply about deploying envoys and making appointments. It could be argued that it is becoming an exercise in networked statecraft that must navigate asymmetrical interdependence, norm diffusion, and competing visions of sovereignty. The concept of 'weaponised interdependence' (Farrell & Newman, 2019, Drezner et al., 2020) highlights how global digital and economic networks create both leverage and vulnerability: actors embedded in central nodes, often large tech platforms or infrastructure providers, can be used to exert pressure, while others seek to hedge by diversifying or reshaping dependencies. This is an imperative that amplifies the strategic salience of the tech diplomats as mediators of both cooperation and resilience-building. At the same time, the EU's tech diplomacy approach to governing emerging and disruptive technologies highlights that influence is often exerted indirectly, by aligning the private-sector behaviour through standards, codes, and collaborative platforms. Conversely, debates over digital and technological sovereignty (Csernaton, 2024d) infuse tech diplomacy with contestations about global tech leadership, strategic autonomy, legitimacy, and future-making: either by promoting a trusted infrastructure and digital rights, or by defending the regulatory space from external coercion, the diplomats translate and negotiate competing visions about what a secure and sovereign digital domain should look like. Moreover, the exportation and global gravitational pull of the EU norms and rules, the so-called 'Brussels Effect' (Bradford, 2020) means that tech diplomacy also functions as a mechanism of normative diffusion, where an engagement with companies becomes a conduit for shaping global regulatory expectations and aligning transnational practices to the European values. In essence, tech diplomacy operates at the intersection of structural network politics, governance mediation, and normative contestation, making it a critical site where the evolving architecture of the digital international relations is both performed and negotiated.

With regard to the means tech diplomats use to advance their objectives, these remain traditional and include negotiation, mediation, and public diplomacy. Also, the tools for engaging with their interlocutors and/or for discussing policies within the scope of their mandate continue to be traditional diplomatic tools for public diplomacy. Besides closed-door meetings, tech diplomats meet their counterparts and other relevant actors in public fora. A representative example is UNESCO's recent set-up of the new Tech Diplomacy Forum, an ad hoc platform bringing together leaders from governments, industry, civil society, and academia. The new forum convened in June 2025, discussing issues at the crossroads between technology, international diplomacy and public policy, including how technologies related to AI, fintech, and space influence geopolitical dynamics and raise concerns about disinformation, cybersecurity, and digital inequality. Tech diplomats therefore negotiate bilateral and multilateral agreements on technological developments, deployment, commercialisation, and use, as well as related horizontal issues, including cross-border data exchange and cybersecurity standards. In doing so, they shape both the national and global

policy and standards. In addition, they discuss digital policy designs and amendments in the light of economic and competitiveness considerations/objectives, that is, based on what their states want to achieve in terms of creating innovative and competitive ecosystems for developing and adopting digital solutions.

The outcomes of tech diplomacy in the international governance of emerging and disruptive technologies are tangible, as evidenced in the work of the UN tech diplomat, which has secured international consensus recommendations on regulating AI in lethal autonomous weapon systems, or the drafting of the UNESCO AI ethics recommendations in 2020. These examples show that tech diplomacy is situated at the intersection between policies regulating the emerging and disruptive technologies and a range of areas, including security and defence, education and health. Similarly, at the EU-level, Gerard de Graff, the EU Senior Envoy for Digital to the U.S. and head of the EU office in San Francisco has been tasked with supporting the tech industry to deal with the EU digital regulations, including the Digital Services Act (DSA) which affects the operations of the Big Tech companies, including Amazon, Apple, Google and Meta in the EU. The DSA outlines the obligations for the digital platforms in areas such as governance, contractual conditions, transparency reporting, information on traders and trading, risk assessment and crisis management, data sharing, auditing and handling disinformation, illegal content, criminal offences and the protection of minors online. These areas of compliance for tech companies are connected to the achievement of broader EU objectives in the digital single market, data privacy rights, and personal safety. Crucially, besides ensuring the U.S. tech sector is prepared for EU compliance, in his post, the EU Senior Envoy for Digital has also used his time to build relationships with the U.S. tech sector.

From a skills perspective, finding the right profile of the tech diplomats is rather challenging, since this role requires a blend of traditional diplomatic skills and the technical and regulatory understanding of the technological tools, developments and their implications, nationally and globally. Tech diplomats find themselves negotiating on a range of issues, from (cyber)security, to economy, data privacy, digital rights, technology standards, and the ethical and security dimensions of emerging technologies, all demanding the capacity to engage with different intermediaries on the inter-relations between technology and state policies across domains, that is, primarily but not exclusively on the digital policies. As a consequence, the skillset of the tech diplomats is at the same time broad and highly technical. More broadly, the tech diplomats must be able to address a vast array of issues under the umbrella of digital policy and technological innovation. For example, the UN under-secretary-general and special envoy for digital and emerging technologies is also the chief executive officer of the International Digital Health and Artificial Intelligence Collaborative project, at the Geneva Graduate Institute of International and Development Studies. The EU Envoy for Digital to the U.S. and head of the EU office in San Francisco has experience in working across a wide range of policy areas, including digital policies, telecoms, cyber-security, standardisation, startups, Greentech, data governance, technology platforms, and international relations. He studied Economic Geography and Regional Planning, European Economy and Law. Though tech diplomats deal mostly with technological innovation and its influence on national and international security and development, their portfolio is broad as the policy areas in which they move are interconnected and interdependent, such as in the cases considering the impacts of the emerging and disruptive technologies, AI, on national security and economic development.

In most cases, this post requires technical knowledge or at least an understanding of the materials underpinning the digital, emerging and disruptive technologies. To provide an example, this paper draws on the first-hand experience of a tech diplomat exchanging with the representative of a Nordic tech start-up developing semiconductors in the EU. Recently, the EU has set ambitious priorities in the semiconductor sector, with the objective of increasing its technological leadership and reducing its dependency on suppliers such as the US and China. An example of this priority setting is the European Chips Act, for boosting EU's competitiveness and autonomy in semiconductor technologies. When discussing with an EU-based tech start-up, the tech diplomat had to be familiar with the technical, regulatory, funding, and geopolitical challenges in the context of which the start-up operated. From a technical level, the construction of semiconductors requires the use of dangerous chemicals. From a regulatory perspective, the use of some of these chemicals, such as PFAS, is heavily restricted in the EU, as opposed to China. From a funding perspective, the European start-ups can receive initial funding more easily, while struggling to ensure the remaining investment needed to further develop their innovation. These conditions make the tech start-ups in Europe look for investments and operations elsewhere, with impacts on the EU innovation, strategic autonomy, geopolitical and economic competitiveness. The tech diplomat in question, therefore, had to be versatile and highly familiar with these areas: research and innovation in semiconductors, EU policy and funding capacities to support start-ups and SMEs, the regulatory ecosystems on the use of chemicals, and how this ecosystem affected or hindered the work of the tech start-up, increasing the risk of competition from China which is willing to provide funding, in return for proprietary rights.

This vignette crystallises the key dynamics of tech diplomacy: it is inherently boundary-spanning, requiring diplomats to possess epistemic agility to translate between technical, regulatory, financial, and geopolitical registers, and to mediate the competing imaginaries of autonomy, competitiveness, and safety. The case also illustrates how the strategic autonomy is negotiated in practice, not as a static goal but as an ongoing balancing act amid weaponised interdependence, where a regulatory stringency such as PFAS restrictions and capital scarcity push firms toward rival jurisdictions, potentially undermining innovation ecosystems unless deftly managed. Furthermore, the diplomat's role exemplifies a multi-level governance understanding, aligning heterogeneous actors, start-ups, regulators, and funders through soft coordination and careful management, thus navigating a fragile ecosystem while projecting credible futures for the European chip sovereignty. Hence, the example foregrounds that the tech diplomacy's effectiveness depends as much on technical literacy and trust-building as on formal policy instruments.

MAIN CONTOURS OF EU TECH DIPLOMACY AS A CASE STUDY

The EU provides another revealing vignette regarding how tech diplomacy is manifested in practice. The EU has emerged as a leading practitioner of tech and digital diplomacy, treating technology governance as a core element of its foreign policy. This shift has been recently exemplified by the EU's new International Digital Strategy unveiled in 2025 (European Commission, 2025), which lays out a comprehensive vision for strengthening international digital cooperation by boosting European competitiveness, safeguarding the digital security of Europe and its partners, and shaping the global technology rules in line with

the EU values. Building on earlier ‘digital sovereignty’ efforts, the strategy moves the EU from ad-hoc initiatives to a more coherent and geopolitical approach. It calls for deepening partnerships through Digital Partnerships and Digital Dialogues around the globe, connecting these efforts via a new ‘Digital Partnership Network’ to coordinate the engagement with like-minded countries. Notably, the strategy also introduces an ‘EU Tech Business Offer’ – a mechanism for jointly mobilising public and private investment and expertise for large-scale digital projects in partner countries, with European tech companies, innovators, and associations working alongside the EU institutions and Member States. Accordingly, this marks a significant evolution in the EU tech diplomacy, as Brussels is exporting regulations and funding, as well as actively integrating European industry into its diplomatic outreach, aligning commercial incentives with foreign policy goals in areas from AI capacity-building for securing the 5G infrastructure.

In parallel to these diplomatic initiatives, the EU has leveraged its regulatory power as a tool of tech diplomacy – with the already mentioned and the so-called ‘Brussels effect’ – whereby the EU rules set de facto global standards. The Digital Services Act (DSA) and Digital Markets Act (DMA) exemplify this influence. The DSA imposes sweeping obligations on Very Large Online Platforms regarding content moderation, transparency, and user rights, while the DMA constrains the anti-competitive practices of the Big Tech as ‘gatekeepers’ (Martens, 2025). Together, these laws signal Europe’s determination to ‘rein in’ the power of the dominant tech firms and assert a human-centric model of the digital economy. More importantly, the EU actively promotes these norms abroad while the EU officials engage counterparts and companies worldwide to explain and encourage the adoption of its standards. In fact, the EU’s tech diplomacy office in San Francisco is precisely to interface with Silicon Valley’s tech giants, ‘unpacking’ the DSA, DMA and upcoming rules for a wary industry. This unprecedented move to station EU diplomats in the heart of the tech industry denotes that engaging directly with tech companies has become a pillar of the EU external action – treating these firms almost as quasi-sovereign geopolitical actors in their own right.

It could be further argued that the EU’s proactive stance on emerging and disruptive technologies further bolsters its tech diplomacy credentials. In 2024, Brussels finalised the world’s first comprehensive Artificial Intelligence Act, a landmark regulation taking a risk-based approach to AI governance. The AI Act strictly curtails high-risk AI uses, from social scoring to real-time biometric surveillance, and mandates transparency and accountability measures, aiming to ensure a ‘trustworthy AI’ consistent with democratic values (Csernaton, 2025). The European officials explicitly frame this as setting a global benchmark for AI, and indeed, other governments are already looking to align with it. In tandem, the EU has pushed forward the Chips Act, enacted in 2023, to boost Europe’s semiconductor capacity and reduce its dependency on foreign microelectronics (European Commission, 2025a). This industrial strategy comes with a diplomatic dimension, namely recognising that securing supply chains for critical technologies is a geopolitical challenge. In this regard, the Commission launched a dedicated ‘Semiconductor Diplomacy Network’ in 2025, the CHIPDIPLO initiative, to strengthen international cooperation on chips. The CHIPDIPLO consortium connects the European industry, think tanks, and policymakers with partners in the U.S. and Asia, facilitating track dialogues on supply chain resilience, reducing strategic dependencies, and coordinating on semiconductor norms and standards. Thus, by embedding tech issues like

AI and chips into its external relations, the EU is leveraging its pursuit of strategic autonomy and using foreign policy tools to bolster control over critical technologies and materials in an era of great tech rivalry. In this respect, the security imperatives are indeed at the heart of the EU's tech diplomacy. The European External Action Service (EEAS) has explicitly linked digital diplomacy (EEAS, 2023) with the international security concerns, asserting that the technological sovereignty in defence and a robust digital ecosystem are prerequisites for Europe's security (EEAS, 2024). Cyber diplomacy has become a prominent component, with the EU's 2020 Cybersecurity Strategy for the Digital Decade and its Cyber Diplomacy Toolbox, a framework for joint EU responses to malicious cyber activities being implemented to bolster resilience against cyber threats (European Commission, 2025b).

On the international stage, Brussels actively advances its vision of a global, open, stable and secure cyberspace through multilateral norm-setting and bilateral engagements. The EU and its Member States have held over 20 international cyber and digital dialogues so far with countries worldwide, from the EU-U.S. and EU-India Trade and Technology Councils, and the Digital Partnerships with South Korea, Japan, and Singapore, to cyber dialogues with India, Brazil and others. Through these channels, the EU shares the best practices on 5G network security, promoting its 5G Cybersecurity Toolbox globally, it coordinates the positions on data governance and internet standards, and it is building capacity with partners to counter cyber threats and disinformation, for instance, funding the cyber training for its Eastern European neighbours (Kurbalija, 2025). The ongoing war in Ukraine has outlined the stakes, with the EU deploying a coordinated cyber response to help Ukraine withstand the Russian cyber attacks, extending its new Cybersecurity Reserve to Ukraine (European Commission, 2025c) and imposing export controls/sanctions to cut off Russia's access to the Western high-tech goods. Hence, technology features prominently in the EU's collective security and defence thinking, from securing supply chains for chips to defending democratic societies against hacking and foreign information warfare.

Another distinctive aspect of the EU's approach is the recognition of the fact that tech diplomacy must engage not only governments but also the private sector as partners in governance. The European leaders increasingly treat Big Tech companies as strategic actors to be engaged via diplomacy, not just regulated or constrained. As noted, the EU's Silicon Valley office is one concrete example, aiming to build direct channels with firms like Google, Meta, Apple, and Microsoft. Moreover, the EU's International Digital Strategy pointedly adopts a more collaborative tone toward industry. Unlike the past EU rhetoric that was often critical of Big Tech, the 2025 strategy notably avoids singling out tech companies for blame, thus omitting, for instance, any mention of the digital services taxes or penalising firms (Kurbalija, 2025). This softening of language signals Brussels' readiness to partner with technology companies in achieving mutual goals, be it combating online misinformation or deploying connectivity in the Global South. Think-tank observers highlight that major tech firms now possess resources and transnational influence rivalling those of many states, so much so that 'technology companies are more than mere players in global politics; they are often the arena itself' (Reif, 2025). By actively engaging Big Tech in dialogue and co-regulation, the EU seeks to harness their innovation capacity and global reach – for example, securing voluntary commitments from platforms to police disinformation and hate speech under the DSA's Code of Practice, and enlisting the companies' help in infrastructure projects, such

as the European vendors Nokia/Ericsson partnering on 5G pilots in Africa. Thus, Brussels' outreach to industry is both pragmatic and strategic, as it acknowledges tech companies as essential allies for issues like cybersecurity, where platforms must help detect and take down cyber threats, and climate change, where tech innovation is needed for clean energy and green IT solutions. In the EU's view, an effective tech diplomacy means that the convening states, international organisations, Big Tech, start-ups, academia, and civil society jointly address the global challenges via a multistakeholder ethos that plays to Europe's strength as a normative power and consensus-builder on the world stage.

Moreover, the EU tech diplomacy is increasingly connected with the broader agendas of sustainability, development, and resilience. The European Commission often refers to twin transitions – digital and green – and in external policy, these efforts reinforce each other. For example, the EU's Global Gateway initiative (European Commission, 2024), a €300 billion infrastructure programme, links digital connectivity investments with climate objectives, such as funding secure broadband networks, data centres, and satellite projects in Africa, Asia, and Latin America that are designed to be climate-resilient and energy-efficient. This involves encouraging sustainable ICT standards, such as advocating for data centres powered by renewables and low-carbon cloud computing and harnessing digital innovation for climate resilience, like using open data platforms for climate modelling, deploying IoT networks for environmental monitoring, and sharing satellite earth observation data to help predict and mitigate climate-related disasters. Practically, this holistic approach means an EU tech diplomat might be equally comfortable with negotiating the spectrum for broadband in a Pacific island state as with discussing AI ethics or critical raw materials for batteries. All these efforts, from cybersecurity capacity-building to climate-tech cooperation, highlight a central theme of the EU vignette. Tech diplomacy, for the EU, is not a separate sphere but a cross-cutting tool for strengthening the strategic autonomy, technological sovereignty and economic security, upholding democratic values, and building resilience against the interconnected threats of the 21st century, whether cyberattacks or climate catastrophes.

Beyond its global external engagements, the EU's tech diplomacy must also account for a significant internal dynamism and divergence. For instance, Central and Eastern Europe (CEE) has emerged as a rapidly growing digital powerhouse, with the 100 largest CEE tech firms boasting a combined market capitalisation nearing \$117 billion and a regional value growth outpacing Western Europe by two to three times over the past decade (Bolanowski, 2025). Yet, this growth is uneven and constrained by structural barriers across the bloc, such as fragmented regulatory implementation, limited access to venture capital, and competitive pressures that push firms to seek external markets or investment (Cotroneo and Derbyshire, forthcoming). The region's substantial human capital and cost advantages coexist with calls from industry for a more synchronised EU-wide level playing field, illustrating the dual imperative for EU tech diplomacy: to integrate and amplify intra-European innovation ecosystems while using normative and financial levers to stabilise and scale the promising actors across the Union. Furthermore, the EU leverages its internal market and diplomatic outreach to bridge regional disparities and bring the European tech companies into a broader strategic engagement. Through targeted dialogues, regulatory guidance, and investment facilitation, Brussels acts as both convenor and enabler, helping fast-growing but fragmented firms scale across borders while aligning them with the European standards and values. This

includes embedding startup ecosystems into Digital Partnerships, thus offering clarity on compliance with the EU rules, and creating channels where industry voices inform external tech diplomacy agendas. Consequently, the result is a dual-track approach: reinforcing the intra-EU cohesion while projecting a united, industry-informed European tech posture abroad.

CONCLUSIONS

Emerging and disruptive technologies, such as AI, quantum computing, blockchain and advanced robotics, have reshaped the global economic structures and challenge the existing security paradigms and power dynamics. The adoption of such technologies at the individual and collective levels has transformed the society radically by creating new ways of working, communicating and delivering services. However, such technologies have also introduced concerns related to cybersecurity, data privacy and new modes of warfare. In this landscape, the tech companies have acquired new power by shaping and influencing trade policies, security and geopolitics. To address these challenges, tech diplomats have been appointed as foreign service officials representing the interests of their country or a group of countries – before tech companies, via dialogue and negotiations. While the Danish Ministry of Foreign Affairs was the first to use the term and introduce an office, this practice has quickly evolved and it has been adopted by other states and international organisations.

The moves of the Danish government and other governments towards appointing tech diplomats is a sign of a structural and significant change in international relations and global governance to which the diplomacy has adapted itself. Diplomacy is being reshaped to meet new challenges posed by digital, emerging and disruptive technologies. The tailored engagement of state officials with their tech counterparts signals a paradigmatic shift in global affairs, international relations, and global governance in at least two interesting ways. First, it signals that the states perceive an urgency to prioritise the policies surrounding the technological developments and their impacts on societies in their own foreign policy agendas. Second, the states consider Big Tech companies as relevant and key interlocutors. The importance of the non-state actors in the diplomatic processes calls into question some central tenets of the classic IR paradigms, which emphasises the inter-state relations in international politics and state-centricity. The work of the tech diplomats in Silicon Valley illustrates the extent to which the economic and technological power assumed and exerted by corporations is also central to international affairs and global governance. This transformation is in line with the position of Keohane and Nye's representation of power as the result of a distributed network of interdependence, rather than being concentrated solely within state institutions.

The rise of the tech companies' influence and new security trends has also led to a broadening in the set of issues covered by the tech diplomats' agendas. Through the years, the objects of discussion between states and tech companies have changed radically, broadening in scope. While the initial discussions focused mostly on economy, security, cooperation, and development, nowadays the range of issues has expanded, covering also data privacy, artificial intelligence, fundamental rights, health, science, research and education, governance, development and sustainable development goals, among others. The widening in scope reflects the states' concerns over the new emerging risks, such as foreign influence, including the influence of the social media (dis)information campaigns, cybersecurity threats, privacy risks, and more broadly, foreign influence and competition.

In terms of future research, this paper provides mainly the perspective of state actors. However, some scholars have also put forward the concept of ‘tech corporate diplomacy’ in reference to the diplomatic efforts of the tech corporations to influence states and international affairs in order to advance their own interests. Future research should address the perceived role of tech diplomats from a corporate perspective.

Acknowledgements

Raluca Csernatonî's contribution to this publication was supported by an EU-funded project, that is the EU Cyber Direct - EU Cyber Diplomacy Initiative at Carnegie Europe.

For their professional support, their comprehensive subject-matter expertise in cyber policy, and their insights into the intricate realm of diplomatic practice - where innovation, defence, public-private relations meet -, Clara Cotroneo would like to thank Christian-Marc Lifländer, Head of Defence Policy Section at NATO

REFERENCE LIST

- Abels, J. (2024) Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations*. 30(4), 842–866. <https://doi.org/10.1177/13540661241260653>.
- Aiken, E., Allen, P., Baudin, A., Finkel, J., Fischer, E., Goldberg, L., Salam, J. and Schmollinger, R., 2025. The Technopolar World: Do Tech Companies Matter as Geopolitical Actors?.
- Bradford, A. (2020) *The Brussels Effect: How the European Union rules the world*. Oxford, Oxford University Press.
- Bradshaw, S. & Howard, P.N. (2018) *Challenging truth and trust: A global inventory of organized social media manipulation*. Oxford Internet Institute.
- Bjola, C. & Kornprobst, M. (2025) Studying Tech Diplomacy – Introduction to the Special Issue on Tech Diplomacy to be published in *Global Policy*, 1–8. <https://doi.org/10.1111/1758-5899.70035> [preprint]
- Barrinha, A. & Renard, T. (2017) Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*. 3(4–5), 353–364. <https://doi.org/10.1080/23340460.2017.1414924>.
- Broeders, D. & Taylor, L. (2017) Does great power come with great responsibility? The need to talk about corporate political responsibility. In: Taddeo, M. & Floridi, L. (eds.) *The responsibilities of online service providers*. Springer, pp. 315–323.
- Broeders, D., Sukumar, A., Kello, M. et al. (2025) Digital corporate autonomy: geo-economics and corporate agency in conflict and competition. *Review of International Political Economy*. 32(4), 1189–1213. <https://doi.org/10.1080/09692290.2025.2468308>.
- Cotroneo, C. & Leonard, S. (2025) The Role of Big Tech Corporations in Military Defence and Civilian Protection: A Case Study of the Russo-Ukrainian War. In: Kwan, C., Gratzner, N., Podiņš, K. et al. (eds.) *17th International Conference on Cyber Conflict: The Next Step (CyCon), 27-30 May 2025, Tallinn, Estonia*. New York, USA, IEEE. pp. 109-125.c
- Cotroneo, C. & Derbyshire, R. Cyber-Attacks against European Critical Infrastructures: solutions for increasing resilience from the tech industry in the EU. To be published in *Journal of Cyber Policy* [preprint].
- Csernatonî, R. (2022) The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty. *European Security*. 31(3), 395–414. <https://doi.org/10.1080/09662839.2022.2103370>.
- Csernatonî, R. & Martins, B.O. (2023) Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics*. 29(3), 849–872. <https://doi.org/10.1080/14650045.2023.224235>.
- Csernatonî, R. (2024a) *Can Democracy Survive the Disruptive Power of AI?* <https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en> [Accessed 20th July 2025]

- Csernaton, R. (2024b) *Charting the Geopolitics and European Governance of Artificial Intelligence*. <https://carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence?lang=en> [Accessed 30th May 2025]
- Csernaton, R. (2024c) *Governing Military AI Amid a Geopolitical Minefield*. <https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en> [Accessed 30th May 2025]
- Csernaton, R. (2024d) *Europe's Wake-Up Call for Tech Leadership*. <https://carnegieendowment.org/europe/strategic-europe/2024/12/europes-wake-up-call-for-tech-leadership?lang=en> [Accessed 30th May 2025]
- Csernaton, R. (2025) *The EU's AI Power Play: Between Deregulation and Innovation*. <https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en> [Accessed 30th May 2025]
- Drezner, D.W., Farrell, H. & Newman, A.L. (2020) *The Uses and Abuses of Weaponised Interdependence: An Overview*. Washington, USA, Brookings Institution Press.
- European Commission (2025) *The International Digital Strategy for the European Union* <https://digital-strategy.ec.europa.eu/en/policies/international-digital-strategy> [Accessed 30th May 2025]
- European Commission (2025a) *CHIPDIPLO Consortium Selected to Support International Diplomacy in Semiconductors*. <https://digital-strategy.ec.europa.eu/en/news/chipdiplo-consortium-selected-support-international-diplomacy-semiconductors> [Accessed 30th May 2025]
- European Commission (2025b) *EU Cybersecurity Strategy*. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> [Accessed 30th May 2025]
- European Commission (2025c) *Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels*. <https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels> [Accessed 30th May 2025]
- European Commission (2019–2024) *Global Gateway*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en [Accessed 30th May 2025]
- European External Action Service (2023) *Digital Diplomacy*. https://www.eeas.europa.eu/eeas/digital-diplomacy_en [Accessed 30th May 2025]
- European External Action Service (2024) *Defence Technologies: Time to Think Big Again*. https://www.eeas.europa.eu/eeas/defence-technologies-time-think-big-again_en [Accessed 30th May 2025]
- Farrell, H. & Newman, A.L. (2019) Weaponised interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351.
- Garcia, E.V. (2022) *What Is Tech Diplomacy? A Very Short Definition*. <https://medium.com/@egarcia.virtual/what-is-tech-diplomacy-a-very-short-definition-9042afdc9ce4> [Accessed 30th May 2025]
- Horejsova, T., Kurbalija, J. & Ittelson, P. (2018) *The Rise of TechPlomacy in the Bay Area*. DiploFoundation.
- Ittelson, P. and M Rauchbauer. 2023. "Tech diplomacy practice in the San Francisco Bay Area."
- Jan Bolanowski (2025) *Tech Firms in Central and Eastern Europe Seek to Catch Up with the West*. <https://www.euronews.com/business/2025/07/03/tech-firms-in-central-and-eastern-europe-seek-to-catch-up-with-the-west> [Accessed 17th August 2025]
- Keohane, R.O. & Nye Jr, J.S. (1973) Power and interdependence. *Survival*. 15(4), 158–165. <https://doi.org/10.1080/00396337308441409>.
- Kurbalija, J. (2025) *EU Digital Diplomacy: Geopolitical Shift from Focus on Values to Economic Security*. <https://www.diplomacy.edu/blog/eu-digital-diplomacy-geopolitical-shift-from-focus-on-values-to-economic-security/> [Accessed 15th September 2025]
- Martens, B. (2025) *Updated Assessment: Memo to the Commissioner Responsible for Digital Affairs*. <https://www.bruegel.org/first-glance/updated-assessment-memo-commissioner-responsible-digital-affairs> [Accessed 15th September 2025]
- de Souza Lima, R.M. and Brito, R.V.L., 2024. War, words, and wealth: exploring the differences between cyber, digital, and tech diplomacy.
- Renda, A., Reynolds, N. & Ronco, S. (2024) *Can the EU Become a Better Partner and Orchestrator in Development Policy? - CEPS In-depth Analysis*. Centre for European Policy Studies (CEPS).
- Kitchen, K.. (2025) *Technology Companies as Geopolitical Actors*. <https://www.gisreportsonline.com/r/technology-geopolitics/> [Accessed 17th August 2025]
- Rauchbauer, M. and Ittelson, P. (2018) *Tech Diplomacy Practice in the San Francisco Bay Area*. DiploFoundation.



Clara COTRONEO is a lecturer and researcher at the University of Leiden's Faculty of Governance and Global Affairs, the Institute of Security and Global Affairs. Her primary areas of research are EU internal security, defence innovation, critical infrastructure resilience and protection, hybrid threats management and resilience management. Her publications have so far focused on cyber diplomacy, defence innovation and critical infrastructure protection. Clara is also a full-time Service Manager at Capgemini Belgium, based in Brussels, for a cybersecurity contract serving 71 European Institutions, Bodies and Agencies. She is also a Senior Fellow at the Global Governance Institute, a Brussels-based think tank where she focuses on AI foresight and technology scanning within the AI Governance Unit of the Institute. Clara has also been a trainer, delivering training activities for prestigious institutions, including the College of Europe and for EU-level training providers, including the European Institute of Public Administration.



Raluca CSERNATONI is a Team Leader and Senior Research Expert at Carnegie Europe in Brussels, Belgium, where she specialised in European security and defence, with a focus on the emerging and disruptive technologies, mainly on new technologies for the EU-funded project called EU Cyber Diplomacy Initiative - EU Cyber Direct (EUCD). She also led Carnegie Europe's research project on 'The EU's Techno-Politics of AI'. Csernatonu is currently also a Professor on European security and defence, focusing on new technologies at the Centre for Security, Diplomacy and Strategy (CSDS) of the Brussels School of Governance (BSoG) and at Vesalius College (VeCo) of Vrije Universiteit Brussel (VUB). At the CSDS, she is also a Senior Researcher on digital technologies for the EU-funded project 'Indo-Pacific-European Hub for Digital Partnerships: Trusted Digital Technologies for Sustainable Well-Being' (INPACE). To that, she is a Co-Leader of the 'Governance of Emerging Technology' Research Group at the Centre on Security and Crisis Governance (CRITIC) of the Royal Military College Saint-Jean in Canada. Between 2022 and 2025, Csernatonu was invited to join the Department of International Relations of the Central European University (CEU) in Vienna, Austria as a Visiting Professor on European security, technology, and the future of warfare. Previously, Csernatonu was a Postdoctoral Researcher and Lecturer at the Department of International Relations of the Institute of Political Studies of Charles University in Prague, Czechia. To that, Csernatonu conducted the research on EU security, defence, and technological policies at the Faculté des Sciences Sociales et Politiques of Université libre de Bruxelles, the Centre for Security and Defence Studies of the Royal Higher Institute for Defence, and at the International Security Information Service Europe in Brussels. She was also a Research Fellow within the Study Program on European Security at the Institute for European Politics in Berlin, Germany. Csernatonu holds a PhD and a Master's degree in International Relations from the CEU. Her academic articles appeared in peer-reviewed journals such as *Minds and Machines: Journal for Artificial Intelligence, Philosophy and Cognitive Science, Global Policy, Geopolitics, European Foreign Affairs Review, European Security, Critical Military Studies, Global Affairs, and European View*. Her co-edited book, *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*, was published with the Routledge Studies in Conflict, Security and Technology Series in 2020.



This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.