ARI 34/2021 (English version)
17 March 2021

Towards a new technology foreign policy line in Spain and the EU

Raquel Jorge Ricart | Fulbright Fellow in Washington, DC (Elliott School of International Affairs), specialising in emerging and disruptive technologies and security and foreign policy | @RaquelJorgeR

Theme

Technology and digital policy need to be converted into a single, sole line of foreign policy in both Spain and other EU member states, as well as at the EU level. The coordinated management of challenges and opportunities derived from digitisation and from emerging and disruptive technologies paves the way for an innovative adaptation of Spain, other Member States and the EU's foreign policy frameworks to the new multilateralism's conditions and needs. This should also serve to update the much-needed anticipation and future scenario techniques driven by foresight exercises, and to strengthen the EU's strategic autonomy both outwardly and –equally importantly– inwardly.

Summary

Technology and digital policy has currently become one of the main global playing fields. However, most States still address technology and digitisation as a purely cross-cutting issue within traditional diplomacy. Technology and digital policy need to be designed, developed and implemented as a singular, unique line of foreign policy. Technology and digital policy is no longer an adjective or corollary to other diplomacies: it is rather a diplomacy in itself. This paper looks at why and how technology and digital policy must materialise into an own unique foreign policy line. To this end, this analysis proposes an actionable-oriented architecture with a vision, mandate, instruments and co-ordination, and its relationship with other diplomacies –eg, scientific–. The case of a European middle-sized power –such as Spain– is analysed as a scalable experience in comparison with other similar EU Member States and in respect to its coherent materialisation at the EU level.

Analysis

It is no straightforward task to convert foreign policy into a truly long-term, whole-of-government State agenda. The three fractures –socio-economic, environmental, and digital and technological– that delineate the current international order pose a challenge to achieve this goal. Spain's Foreign Affairs Minister, Arancha González Laya, highlighted this urgency during her appearance before the Congress of Deputies in February 2020, when she laid down Spain's main foreign policy guidelines.

Building upon these three fractures, digital and technology governance features a pressing trait: the speed, scope, intensity, and dispersion of digital transformation far

outpace most countries' current anticipation and management capabilities to respond to its challenges in a safe, secure and sustainable manner. Even multilateralism is not yet fully adapted to the impacts of technologies and digitisation on every multilateral layer: from economy (data standardisation, cross-border data flows and supply chains) to human rights or humanitarian affairs. In addition, there is a growing social malaise due to the lack of a response of public-led tools to digitisation-driven challenges –such as labour market adaptation or industrial competitiveness. The mistrust of public opinion in institutions and the subtle, weak signal of a loss of the sense of community –due to disinformation and an increasing individuation– further reinforce the imperative for an own, unique line of technology diplomacy as a core issue.

This patchwork of ruptures, accelerations, curbs and overlaps give rise to a need for such a singular line of diplomacy within all Member States and in the EU's foreign policy frameworks. However, this is not only about creating a new line with specific, actionable measures and instruments. It is also about rethinking the very sense and understanding of how overall foreign policy must work in the 21st century, with both an outward and an inward focus.

This requires the creation of organisational ways of proceeding, institutional figures, new and adapted communication and coordination channels, capacity building and development, and –importantly– confidence-building measures across all stakeholders involved in technology and digital issues. Public agencies, the private sector, civil society, cities and cross-border economic clusters have not always been used to work altogether.

Alongside this multi-stakeholder perspective, this policy paper points out the extension of current works on cyber diplomacy to the digital and technological arena –both jointly and separately, depending on the subject-matter–. Secondly, this paper makes a distinction between scientific and technology diplomacy: both are intertwined, but their realities and mechanisms are too specific and singular. Scientific and technology diplomacy may certainly work together on issues such as outer-space policy, but scientific diplomacy cannot respond to digital human rights, humanitarian technologies, military AI, Big Tech company regulation or international norms and confidence-building measures on cyber or Smart Cities.

(1) Technology and digitisation as foreign policy

Ursula von der Leyen, President of the European Commission, recognised in her State of the Union Address of September 2020 that 'Europe has been too slow and is now dependent on others'. Unless Europe starts leading on its own digital pathway, it 'will have to follow the way of others, who are setting these standards for the EU'. To this end, the EU needs to work on its own technology diplomacy both outwardly and inwardly. The European Digital ID, or Just Transition Funds and Digital Europe Programme within the Recovery Plan and NextGenerationEU budgets are also foreign policy, but inwardly. They do look forward to increasing and structuring Member States' capabilities to work with one another, and strengthen endogenous capacities. This may build up a robust, joined-up framework to potentially launch a digital and technology diplomacy strategy.

The first-ever EU Foresight Report –released in the same month as Ursula von der Leyen's State of the Union Address– devotes a great portion of its content to how to reduce technology dependence from third countries on several fronts. The EU produces only around 10% of global production of advanced components for data processing –in particular microprocessors–, which makes EU supply chains highly vulnerable. The EU similarly relies heavily on third countries for critical raw materials, such as graphite, lithium and rare earths. They are essential elements to bolster the EU's strategic autonomy in green technologies, batteries, solar and wind energy or hydrogen. In order to achieve the EU's goals it will need 18 times more lithium by 2030 and 60 times more by 2050.

Once technology diplomacy has been appropriately settled inwardly, the second step –which must be conducted simultaneously as well– is to focus on outward technology diplomacy. At present, the EU has put the focus on finding its own space away from the growing China-US rivalry. The EU is working towards this with many tools, such as regulations on Big Tech –the Digital Services Act (DSA) and the Digital Markets Act (DMA)–, secondly, on a new cybersecurity package –including critical infrastructures, an updated NIS Directive, a Cybersecurity Strategy and other documents–, and, thirdly, institutional responses to like-minded partners' activities –such as the US-led Clean Network programme or new EU-led platforms, such as GAIA-X, which has ended up embracing non-EU companies.

However, the EU has not yet consolidated an own line to internationalise what may be its first test of technology diplomacy. Building upon the 'Sinatra Doctrine' promoted by Josep Borrell, High Representative of the EU for Foreign Affairs and Vice-President of the European Commission, the EU style must become the *modus operandi* in global technology governance. China is gaining large Smart and Safe Cities contracts –such as Huawei's US$172.5 million megaproject with Nairobi (Kenya). This may make the EU get left behind, despite the fact that the recently released EU-Africa 2020 Roadmap ranks digital transformation second in the priority agenda. The same situation may happen with China's Digital Silk Road, which has invested more than US$17.000 million in optic fibre cables, e-commerce and or data centres since 2013.

It is important to note that this issue is not only about China and the US. The EU must look forward to higher levels of cooperation with other countries in other regions, such as Latin America and the Caribbean, Africa and South-East Asia. This might happen at international forums where the EU, which promotes an open, free and safe Internet approach or international norms on cyber, falls back on the support from countries such as Brazil, India and South Africa. These three BRICS decided not to sign a Sino-Russian led Code of Conduct on State responsibility in the ICT.

Despite these efforts, the European model is not yet able to offer a robust, joined-up, coherent approach across all countries. It is true that it is increasingly opening up new avenues on technology diplomacy, such as the Global Democratic Alliance for AI, or the slow inclusion of humanitarian technologies within the EU development cooperation agendas and crisis management scenarios (such as the Copernicus satellite). However, internationally, technology is still balkanised. There is a growing assertiveness towards non-democratic proposals at international forums; non-democratic countries are

collaborating at a more rapid speed than democratic countries (such as Sino-Russian military technology cooperation); and seats in the highest spheres of power and decision-making are being occupied by experts from non-democratic countries in strategically relevant international organisations for technology and digital issues, such as the International Telecommunications Union and the UN Industrial Development Organisation.

As the High-Level Experts Group on Digital Cooperation at the United Nations highlights, multilateralism relies on interconnectivity, respect and protection in the digital era, under the principles of freedom and equality. Hence, the importance of having a robust, coherent technology diplomacy framework to work on the promotion of digitisation as a global commons, digital capacity building-up and the protection of human rights in the digital era.

(2) How to integrate the dispersed into a single framework

The tear 2021 appears to be an opportunity to reconfigure the foreign policy architecture; to convert technology and digital policy into foreign policy; and to acquire relatively greater influence in both aligned and non-aligned countries, as well as regional cooperation systems. The reasons are as follows:

(a) Technology and digital policy blur the traditionally dichotomous vision between geopolitics and public policies. This hybrid opens up a greater involvement of new actors into a country's –or the EU's– foreign policy action. This may be reflected with many examples, such as the interaction of diplomatic delegations with the private sector when these companies can provide quick information on Internet shutdowns during an election day or street protests in a country that is of strategic interest. Another example is the new demands for economic intelligence by European multinational companies which need closer collaboration with governments and information on technology geopolitics in the area they aim to invest in. Even more, the very image and reputation of a country relies on forwarding a solid message and strategy on such an important issue, through a Mission-Country Approach (or Mission-EU Approach).

(b) Social, political, economic, environmental and cultural challenges that foresee exercise needs to address also permeate with the digital. This makes technology become an issue which is no longer cross-cutting or a corollary to others. Due to increasing disinformation campaigns, the EEAS –European External Action Service– set up a cooperation framework between Member States and the Strategic Communications Working Group within EEAS, through the Early Warning System and with Points of Contact. For example, the case of Spain reflects how important it is to institutionally structure management and response to disinformation campaigns: it has been centralised under the National Security Council (CSN) since November 2020, which is the principal advisory body that reports to the Prime Minister. It falls back on the 2018 Disinformation Action Plan. The purpose is dual: first, to combat disinformation; secondly, to guarantee Spain's image, reputation and credibility vis-à-vis false news. This entails

dialogues with representatives from media and civil society, as they experience this reality first hand.

(c) There is a need for the creation of a Special Representative for Global Digital Affairs within the EEAS. Currently, digital policy is mainly managed by both the Competence and Single Market Commissioners and it sometimes entails slow or divergent ways and means to respond to crises or other scenarios. This reveals the urgency of 'strategising' the work outwardly under the new figure of a Special Representative in both the European Commission and in all Member States' Ministries of Foreign Affairs, with no exception.

Each country needs to strategise its most pressing interests to adapt the mandate, vision and instruments of this Special Representative. For example, in the case of Spain, there are several reasons to shape the structuring and content of this new technology diplomacy: Spain is the leading country in 5G Smart City pilot projects; it is to be the entry point of Google-led *Grace Hopper* submarine cables towards Europe; Spanish companies are to create a significant number of in-country data centres; and lessons drawn from previous candidacies to lead strategic centres, such as the European Cybersecurity Centre.

(3) Materialising the new architecture of digital and technology foreign policy

The example of Spain will serve to show how materialising a new technology diplomacy line within a European middle power may be scalable to other EU Member States. Most EU countries are similarly middle powers. This analysis is strategic for both inward and outward technology diplomacy in the European territory, at the EU-wide and Member State levels.

With the presentation of Spain's new Foreign Policy Strategy for 2021 and beyond, the Spanish Ministry of Foreign Affairs announced the drafting of a new Strategy on Global Order and Technology. This policy paper articulates the three main axes that the strategy requires: vision, mandate (institutionally and in capabilities) and coordination (inwardly as a country and outwardly with the EU, other Member States and like-minded partners).

(3.1) Vision

Vision is the bedrock of technology diplomacy. As Spain's Minister of Foreign Affairs highlighted, it is essential to turn foreign policy into a truly long-term, whole-of-government State policy. To this end, technology diplomacy must be enduring in time (regardless of electoral cycles and political colours in power), sustainable in capacities, feasible and consensus-based.

To be enduring in time and feasible, Spain's National Office on Foresight and Long-Term Strategy –which directly reports to the Prime Minister– plays an essential part. Technology foreign policy is far more domestic than it seems at first sight. It heavily relies on a robust methodological analysis of challenges, opportunities and mega-trends within a country to go ahead, with anticipatory governance and prevention measures in the long term.

In order to internationalise what is internal to a country, it needs to make digital transitions within its territory. This is the example of Telefónica's efforts to bridge 100% of the territory using fibre-optic cables and 75% of Spain using 5G networks by the year 2025. The government released its 2025 Digital Spain agenda in July 2020. According to this programme, it looks forward to mobilising €140.000 million for Spain's digitisation until 2025. A technology foreign policy line will be truly actionable and results-oriented if Spain is first capable to work towards achieving its in-country goals: widen the 5G spectrum up to 100% of the territory –now it accounts for 30%–, reskill and train in digital skills up to 80% of workforce, set up a National Charter on Digital Rights and transit towards a data economy where 25% of companies use Artificial Intelligence and Big Data. This should allow subsequent technology diplomacy in areas ranging from the political and economic, to social, development cooperation, public diplomacy, and defence and security diplomacies, in a sustainable, sustained, robust and credible manner vis-à-vis third countries.

For the vision to be consensus-based, there are two main actions to be conducted. First, technology diplomacy must be able to resolve institutional and sector-based divergences vis-à-vis the emergence of a 'one-stop' technology diplomacy framework. This is important because technology diplomacy is also inward diplomacy: how to structure what is happening within a country or the EU. To reduce these risks, an important step is to set up a technology diplomacy based on dialogues and constant public consultations with all stakeholders which are involved in technology and digital issues directly or indirectly –such as energy or environmental companies–.

Because technology diplomacy will be intrinsically interconnected to national strategies, Spain's MFA –and other countries' MFAs– will need to closely work with the corresponding National Office, Department or Agency on Foresight. This should help ensure dialogues with all sorts of stakeholders in order to anticipate and plan how to internationalise the country's ideas (economically, but also politically and geopolitically) according to the possible, potential, plausible and preferable future scenarios. To this end, it will be important to understand the distribution of competences within a country –for example, in Spain there are some shared or decentralised competences with regional governments–. This is especially strategic in 2021 and onwards, as the EU Recovery Plan and NextGenerationEU funds will help step up this mission.

(3.2) Mandate: institutional learning and capacity building

The second axis is mandate. This has two main pillars: a complex institutional structuring (organically) and capacity building (new capacities and adapted ones). The case of Spain offers some lessons for other European middle powers on how to materialise this mandate.

With regards to institutional structuring, the so-called digital and technological fracture in the global order is addressed by the National Security Department (DSN), which directly reports to the Prime Minister –particularly in the Cybersecurity National Council–. It addresses risk and threat mapping, analyses possible crisis scenarios and contributes to resources availability and coordination, among others.

However, this dimension (coordination, verification and planning) must be accompanied by specific teams and departments responsible for execution of technology diplomacy as such –as a whole-of-government issue in a coordinated manner–. This specific execution task will be capable of better effectively addressing the positioning of the country or the EU as a country/Union of reference in multilateral negotiations, as well as a robust, coherent, joint-up voice when it comes down to discussions about international normative regimes related to technology diplomacy, such as human rights law or Responsibility to Protect. To this end, the Directorate-General for Coherence, Strategy and Foresight within the Spain's State Secretariat on Global Spain –which pertains to the Ministry of Foreign Affairs– might be useful to centralise technology diplomacy actions, while coordinating with the National Security Department, the Secretary of State on Digitisation and Artificial Intelligence (SEDIA, which belongs to the Ministry of Economic Affairs), the Ministry of Industry, the Ministry of Science and Innovation, the Secretariat for Defence Policy, the Vice-Presidency on Ecological Transition and Demographic Challenge, and the National Office on Foresight and Long-Term Strategy. This is scalable to institutional learning realities from other European middle powers.

In the case of the European Commission, this technology diplomacy line may be scalable with its centralisation at the EEAS, and the necessary coordination with the Commissioner for Foresight and Inter-institutional Relations, as well as the Commissioners on Competence and Single Market.

Alongside this institutional restructuring, there is a need for a new Special Representative on Global Digital Affairs. In the case of Spain, the MFA appointed its first Ambassador-at-Large on Special Mission for Hybrid Threats and Cybersecurity in 2020. However, technology and digital policy exceeds the scope of cybersecurity, and Spain –as well as other Member States and the EU– should have a specific figure of Technology Ambassador, alongside the current Ambassadors on Cyber Issues.

Denmark was the paradigm country to create this figure of Tech Ambassador in mid-2017. The objective was to increasingly influence its international agenda and its own preparedness in issues such as Artificial Intelligence, the future of work, personal data protection, social media and democracy, crypto-currencies in the global financial architecture, or combating terrorism online, and digital taxation. With offices in Beijing (China), Copenhagen (Denmark) and Silicon Valley (the US), the Tech Ambassador works hand in hand with diplomatic delegations, but manages the mandate autonomously. This means that the Technology Ambassador works with a three-speed approach: by creating new sector-based alliances; by participating in multilateral forums with States; and by promoting and developing multi-stakeholder schemes.

The fact that the Technology Ambassador is responsible for the international presence and influence of his country's or the EU's mission on disinformation, digital taxation, data ethics and AI, digital human rights or other issues, certainly gives legitimacy and credibility, as occurs with France's Directorate-General for Cybersecurity Strategic Affairs within the MFA. The reasoning is that it is seen as a whole-of-government approach –regardless of whether internally each topic is more centralised in one or another department or agency, depending on the nature of the topic (ie, digital taxation

will not be managed by the same agency as military AI). It provides the country or the EU with higher levels of coordination, evidence-based policymaking and, especially, accountability instruments on what has already been done, what lessons may be drawn and how structured the next step should look like.

While other country-case experiences might offer inspiration, each country –especially mid-power countries such as Spain and a large set of EU countries– needs to adapt its own figure of Technology Ambassador *sui generis*, according to its own in-country realities. The reasons are as follows:

(a) Each country will have to decide whether the Technology Ambassador is accompanied by a larger or smaller team, depending on the needs and the scope of its goals. Equally important will be the type of Ambassador: whether a fixed Representative (permanent, with an executive role, having an own department or Directorate-General within the EEAS, or directly reporting to the HR/VP), an Ambassador-at-Large or Special Envoy (higher level of independence, but without a large team and functions not usually execution-oriented), or other figures.

In the case of Spain, an Ambassador-at-Large or on Special Mission is not enough. This might be useful at the beginning of the technology diplomacy launch but, in any case, it should transit into a more executive role afterwards, with a fixed Special Representative for Digital Affairs. The same case applies to the EU. While in Spain's case the figure of an Ambassador for Cyber and Hybrid Threats already exists –although a new Tech Ambassador figure should be created–, the EU has none in either case.

A Special EU Representative for Global Cyber and Digital Affairs should be created. This would reduce transaction costs between the EEAS and the Member States on diplomatic decision-making and influence internationally, centralise the coordination, effectiveness monitoring and execution of EU policies, and streamline the interaction within the EU (between Commissioners or agencies such as ENISA, EUROPOL, EDPS…), and between the EU and like-minded partners (EU-NATO, EU-African Union, EU Diplomatic Delegations…). In any case, the Ambassador should require a group of people specialised in both 'content' (issues) and 'continents' (functions) to make technology diplomacy move forward.

(b) Priorities in foreign policy and existing capabilities differ. In the case of Spain, the last 2015 Foreign Policy Strategy highlighted four priorities: coherence, efficacy, and transparency in foreign action; to promote and project the country's values and interests; to place the citizen at the centre of the foreign action agenda; and to project Spain globally as an advanced country. Incoming Foreign Policy National Strategies should include technology and digital affairs –or technology, digital, and cyber affairs, if the latter has not yet been included– as an own line of foreign action, alongside other issues such as Rule of Law, fight against poverty, development cooperation, arms control, stronger Europe, climate change, language and culture, and region-based focus.

(c) Bilateral relations matter. The Technology Ambassador mandate should also be adapted to existing bilateral relations. In the case of Spain, the Ambassador should not overlook Spain's priorities with Latin America and the Caribbean. Interests with Latam are equally scalable to technology policies.

(d) The agenda needs to prioritise the issues in which the country or the EU has a comparative advantage, or where it is leading an innovative pathway within the digital world. A clear example of this aspect is Spain's leading action towards a cohesive, solid Charter on Digital Rights.

(e) The Tech Ambassador needs to abide by the principle of professional integrity and ethics during his duties, as well as after his mandate (sensitive information non-disclosure), as the Ambassador would be working hand in hand with companies.

In any case, regardless of which particularities appertain to the Tech Ambassador in each European middle power or at the EU level, all of them should be oriented to achieve two EU objectives: strategic autonomy and resilience for a sustainably green, social and digital Europe.

(3.3) Coordination (inwardly and outwardly)

In order to move forward a sustainable, sustained, feasible and consensus-based foreign action, with a mandate and a structuring made up of institutional development and capacity building, coordination is essential.

Outwardly, the EU's Cyber Diplomacy Toolbox must comprise this cyber sanction regime –against government-backed cyber operations against EU members and institutions, attacks on critical infrastructure, cyber-espionage and intellectual property theft, among others–. But it should also include larger teams specifically specialised in cyber, technology and digital diplomacy, both within the EEAS and in EU diplomatic delegations abroad. The day-to-day diplomatic activity needs specialists who are able to channel technology diplomacy as a singular line of discussions –and not just as a cross-cutting or corollary topic to other diplomacies–. This is especially important for the EU as regards the ground work in its Delegations at international organisations –in Vienna, Geneva and New York City–, in the US, in China and in other regional organisations –the African Union, ASEAN and in Latin America and the Caribbean–.

If the EU aims to ¡speak the language of power' and materialise its technological sovereignty, then it needs to structure its outward diplomacy in 'content' (cyber sanctions regime, stronger voice in international discussions on data standardisation, cross-border data flows, international humanitarian law and disruptive technologies) as well as in 'continent' (specialised experts, Regional Bureaus or subject-matter offices, Public Diplomacy…).

Inwardly, a technology foreign action strategy should look forward to its mandate coordination with EU institutions –Commissioners (Competence, Single Market), Directorate-General (Research and Innovation, DG CONNECT, IDEA) and Service Departments (Foreign Policy Instruments)–, but also its coordination with European

legislation, so this diplomacy falls back on cohesive regulation which has already been written for related topics, such as development cooperation –humanitarian technologies– or trade –by adapting new digital-related trade to these clauses–. An example of this in Spain would be the inclusion of new technology-related operations in the Foreign Cooperation Units and ICEX Offices (international trade offices abroad).

This would allow each delegation to devote greater or smaller efforts to specific topics within the technology diplomacy world, depending on the priorities within each delegation: should the delegation focus on satellites, submarine cables, crypto-currencies, Internet of Things, AI, 5G and cybercrime (online child exploitation, financial sector)? Or should it shift the focus onto larger amounts of resources dealing with lethal autonomous weapons systems, or e-Government training for local actors?

That being said, this is not only about technology diplomacy having to adapt to traditional diplomacy, but it is also about traditional diplomacies having to understand the new line of technology foreign action. Hence, it is important to distinguish between scientific diplomacy and technology diplomacy. In the case of Spain, both are embedded within the Report on Scientific, Technology and Innovation Diplomacy. This was a worthy effort in the 2010 decade. However, both science and technology have evolved differently, and they need differentiated lines. Scientific and technology diplomacy may certainly work together on issues such as outer-space policy, but scientific diplomacy cannot respond to digital human rights, humanitarian technologies, military AI, Big Tech companies' regulation or international norms and confidence-building measures on cyber or Smart Cities.

Effective coordination of technology governance means responding to the following dilemmas:

(a) Whether it opts for cross-cutting governance or for a technology-specific governance (the former would be the most appropriate).
(b) Whether technology must be governed vertically or horizontally.
(c) Whether the technology-global order nexus must be addressed with *ex ante* measures (preventive, anticipatory) or *ex post* (punitive).
(d) Which ways and means should be set up to engage non-state actors (private sector, social sector and civil society) into decision-making processes.

Conclusion

Global technology governance is still unfolding. There are more questions than answers. However, this should not deter any country or the EU from establishing an own, singular line of foreign action devoted to emerging and disruptive technologies, and digitisation. This is a timely opportunity: in content and in 'continent'. Some European countries have been developing the first steps towards this technology diplomacy. However, it is not yet enough. The case of Spain offers some reflections on how to materialise this technology diplomacy in the so-called 'European middle powers'. This actionable-oriented architecture may be scalable to other EU countries. It may serve as well for the very EU level to decide how to establish a new technology diplomacy framework both outwardly and inwardly.

First, the internal structuring of a Country-Mission Approach is necessary for an issue such as technology and digital affairs whose nature far outpaces most countries' capabilities to respond to its challenges in a safe, secure and sustainable manner. This would trigger better anticipation and prevention tools upon crisis scenarios, at all layers: the purely political layers (AI challenges for democracy), security challenges (cybercrime, autonomous lethal weapons systems, human rights regimes) and economic priorities (industrial competitiveness and critical raw materials supply chains).

Secondly, if European middle powers are able to structure and adapt their own technology diplomacy framework to their comparative advantages, then these countries and, by extension, the EU, might increase their presence and influence in the definition and negotiation of international issues at the multilateral level. It is true that some great powers have a privileged position, such as China and the US. However, if European middle powers step up their capabilities and technology diplomacy frameworks, this would help the EU to scale up efforts at the multilateral level. This effort would in turn help Spain to step up its influence in decision-making processes which are held within the EU.

Third, technology and digital policy blurs the traditionally dichotomous vision between geopolitics and public policies. Technology foreign policy is far more domestic than it seems at first sight. It heavily relies on a robust methodological analysis of challenges, opportunities and mega-trends within a country to go ahead with anticipatory governance and prevention measures in the long term. This might lead to new organisational culture approaches within a country where the private and public sectors have not always been used to work altogether.

It is true that it is not a straightforward task to turn scattered, tactical policies into a whole-of-government, strategic approach. However, existing efforts are worthwhile and they may serve as lessons to start materialising what a truly technology diplomacy means. The COVID-19 pandemic and trends in these past years, there is an opportunity to structure these scattered initiatives into a single, unique line of technology and digital foreign action. If the EU and its Member States aim to speak the language of power as well as gain terrain in the multilateral order, then the building-up of a coherent, robust, solid, feasible and sustained architecture of technology diplomacy is the next step to work on. Strategic autonomy and a sustainable digital, green and social Europe will rely on it.