The Era of Digital Foreign Policy: Comprehensive Approaches to Digitalisation

ABSTRACT

As the theme of this issue, ‘foreign policy for the 4th industrial revolution’, suggests, diplomats and foreign ministries are faced with tremendous changes brought about by digitalisation. The ability to respond to these changes appropriately and effectively determines the future prosperity of countries. Foreign policy is already digital in many ways - including its tools and the topics on bilateral and multilateral agendas. In this article, we introduce the idea of ‘digital foreign policy’ as a comprehensive way of responding to the challenges of digitalisation and the 4th industrial revolution. We argue that the comprehensive approach called for by ‘digital foreign policy’ is best captured by...
1. What is digital foreign policy

Discussions around digitalisation, diplomacy, and international relations tend to focus on the ‘transformative impact of new communications technologies’ (Cornut & Dale, 2020) or the ‘use of digital media in the field of diplomacy’ (Adesina, 2016). A lot has been written about the use of social media in diplomacy and in particular as a public diplomacy tool (Bjola & Holmes, 2015; Manor, 2019). Yet, digitalisation is not only about bringing new tools to diplomatic practice. It changes social and political relationships and brings about new questions that call for governance at an interstate and global level.

Further, it is abundantly clear that the impact of digitalisation on diplomacy and foreign policy is no longer limited to siloed policy areas or specific practices. Debates and negotiations are no longer confined to technical questions dealt with by technical and standardisation organisations. The available digital practices and tools go far beyond the use of social media. Up until a few years ago all ministries of foreign affairs had addressed the digitalisation of foreign policy and diplomacy in a piecemeal fashion. Given the importance and impact of digital on diplomacy, such a piecemeal approach seems less and less effective.

The term digital foreign policy encompasses the realisation that all aspects of diplomacy and foreign policy are impacted by digitalisation and its consequences and that a comprehensive and coordinated approach

Key words: digital foreign policy, digital diplomacy, digitalisation.
is needed in the face of accelerated digitalisation processes and their impacts.

In order to provide this comprehensive approach, our way of framing digital foreign policy consists of a three-part typology. Each part of this typology describes an area of diplomacy and foreign policy in a digitalised world. The chance of thinking in terms of digital foreign policy lies in not treating these areas in silos but in understanding them as a coherent whole. Digital foreign policy consists of:

- digital as a topic for diplomacy and foreign policy
- digital as a tool for diplomacy and foreign policy
- digital as something that impacts the geopolitical and geoeconomic environment in which diplomacy is practised and foreign policy is conceived.

Some of the digital topics on the global agenda include: Internet infrastructure centred around global connectivity standards and strategies, e-commerce policymaking, cybersecurity, and human rights (including the protection of privacy and freedom of expression). These topics are dealt with by some international organisations traditionally associated with digital topics such as the International Telecommunications Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN). Digital topics have also entered new spaces, including the World Trade Organisation (WTO) and the United Nations Human Rights Council (UNHRC). This also means that digital topics are sooner or later something that all diplomats, no matter their particular area of focus, need to be able to address effectively. The UN has also started to address these issues in a more comprehensive way as signalled by the UN Secretary-General’s Roadmap on Digital Cooperation.

Examples of digital tools for diplomatic practice include the introduction of email to the daily work of diplomats (Kurbalija, 1997) and the use of websites by ministries of foreign affairs and international organisations (Kurbalija & Baldi, 2000). This also includes digital knowledge management tools that build on the digitisation of key documents and their searchability (Kurbalija, 1997). More recently, big data and artificial intelligence have been explored as tools for diplomats (Rosen Jacobson et al., 2018; DiploFoundation, 2019).

When it comes to the geopolitical and geoeconomic environment in which diplomacy is practised, there is perhaps no more tangible example than to look at the network of fibre optic cables that spans the world. This network of cables forms part of the infrastructure that underpins almost all aspects of our societies and economies. Geopolitics becomes no more
obvious than in the confrontation between China and the USA on various tech issues, such as the so-called ‘AI arms race’.

2. Comprehensive digital foreign policy strategies: An overview

A comprehensive digital foreign policy strategy can be defined as ‘a strategy document that outlines a country’s approach to digital issues and digitisation in relation to its foreign policy. It touches on numerous digital issues and connects the dots between the ministry of foreign affairs and various other ministries and key stakeholders. It also outlines areas of policy priorities in regard to digitalisation and how these priorities are pursued as part of the country’s foreign policy’ (DiploFoundation, 2021)

At the time of writing only five countries have released comprehensive digital foreign policy strategies. These are Australia, Denmark, France, the Netherlands, and Switzerland. Other countries have taken different approaches. In some cases foreign policy strategies include sections on digitalisation and digital topics, in particular cybersecurity. In other cases countries have digital strategies that touch on foreign policy aspects. In addition, countries’ cybersecurity strategies and national AI strategies, to name just two examples, are also giving insight into aspects of digital foreign policy. Lastly, foreign ministries are informing on aspects of their digital foreign policy on their websites.

It is important to stress that we are not arguing that all countries need to develop comprehensive strategic documents along the lines of these existing five strategies. Rather, we argue that as countries search for ways to practice effective diplomacy and foreign policy in relation to digitalisation and the emerging challenges associated with the 4th industrial revolution, these documents can serve as a useful point of reference. We analyse them in the following:

• France published its ‘Stratégie internationale de la France pour le numérique’ in 2017 (Ministère de l’Europe et des Affaires étrangères, 2017). The strategy covers digital governance, economy, development, and security. On the normative side, the document stresses the importance of an open and inclusive digital international environment,
the promotion of universal access to diverse digital technologies, and the need to build trust on the internet.

- The Dutch Ministry of Foreign Affairs released its ‘Digital Agenda for Foreign Trade and Development Cooperation’ strategy in 2019, as a follow-up to the 2018 Dutch Digitalisation Strategy. The strategy focuses on four priority areas: (a) digitalisation and the Netherlands’ international position, (b) digitalisation for development, (c) digital security and freedom online, and (d) digitalisation in the trade system. The strategy emphasises the need to cooperate internationally in order to benefit fully from the opportunities of digitalisation.

- At the end of 2020, Switzerland published its ‘Digital Foreign Policy Strategy 2021–24’, which is a follow-up to the ‘Swiss Foreign Policy Strategy 2020–23’. There are four areas of priority: (a) digital governance, (b) prosperity and sustainable development, (c) cybersecurity, and (d) digital self-determination. The strategy aims to ‘raise Switzerland’s profile in the area of digital governance, further develop its digital foreign policy and position International Geneva as a prime location for discussing digitalisation and technology’ (FDFA, 2020).

- Denmark released its ‘Strategy for Denmark’s Tech Diplomacy 2021-2023’ in early 2021. The strategy is structured along three pillars: responsibility, democracy, and security. It aims for a more inclusive, sustainable, and human-centred technological development.

- Australia published its ‘International Cyber and Critical Tech Engagement Strategy’ in spring 2021. This strategy comes after the initial ‘Australian International Cyber Engagement Strategy’ of 2017 and the 2019 progress report. The strategy is structured along three main areas: (a) values, (b) prosperity, and (c) security. The values include democracy, human rights, ethics of critical technology, and diversity and gender equality.

Analysing these five strategies in a comparative perspective, five key observations emerge. First, there are differences in terminology, which need to be taken into account. Second, the strategies cover a broad range of similar topics but do show diversity in their particular emphasis. Third, all strategies navigate a space between competition and cooperation. Fourth, capacity development is mentioned in all strategies and plays a prominent role in some. Fifth, all strategies touch on aspects of coordination, institution-building, and personnel. We look at these five observations in greater detail in the following.
First, while the strategies share a number of similarities and do touch on similar topics, they do not always speak the same language. Differences in terminology are noticeable, as indicated by table one. When it comes to digital foreign policy, digital diplomacy, and Internet Governance, there is a great variety in the terminology used. Within these debates, we typically encounter a number of different prefixes such as e-, net-, cyber-, digital-, and tech-. These are sometimes used interchangeably, but when analysed more closely, certain prefixes reveal particular connotations (Kurbalija, 2015). For example, typically, the pre-fix cyber is associated with a focus on security. The e-prefix is most often found in connection with commerce and education. Tech- is a prefix more closely associated with the business sector and technology and gained particular prominence after Denmark created the position of Tech Ambassador in 2017.

Table 1 The use of prefixes in five digital foreign policy strategies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of total words</td>
<td>23,213</td>
<td>4,051</td>
<td>23,285</td>
<td>10,753</td>
<td>18,177</td>
</tr>
<tr>
<td>cyber</td>
<td>425</td>
<td>13</td>
<td>66</td>
<td>25</td>
<td>89</td>
</tr>
<tr>
<td>online</td>
<td>81</td>
<td>1</td>
<td>16</td>
<td>28</td>
<td>12</td>
</tr>
<tr>
<td>digital</td>
<td>82</td>
<td>37</td>
<td>312</td>
<td>209</td>
<td>223</td>
</tr>
<tr>
<td>virtual</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>net</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tech</td>
<td>14</td>
<td>77</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>11</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Source: DiploFoundation

The Australian strategy is framing the topic mainly through reference to cyber. This is used in the sense of cyber security but also used to describe the realm that the strategy applies to: cyberspace. In contrast, Switzerland uses the term digital to describe the realm that the strategy applies to. The Swiss strategy also offers a clear definition in this regard: ‘Digital space not only includes networks and devices, but also the relevant actors, various processes and interactions. In the same way as land, sea and air are considered ‘spaces’ [...] the digital space is also considered a new dimension which extends beyond national borders’ (FDFA, 2020, p. 3). France and the Netherlands place similar emphasis on using ‘digital’ as the main way to frame the debate. In contrast, Denmark prefers to frame its digital foreign policy strategy around the term tech diplomacy and a focus on the role of tech companies is evident.
What is noticeable from these selective examples is that cyber, digital, and tech are almost used interchangeably. Yet, they do reveal subtle differences in emphasis. While we do not argue that countries should work towards greater terminological coherence, this diversity in terminology can create additional challenges. These challenges include (a) potential confusion for governments, companies, and other stakeholders regarding the topics under discussion, (b) resources being wasted and opportunities for synergies lost, and (c) greater difficulties in overcoming policy silos or reaching multilateral agreements (Kurbalija, 2015).

Second, in terms of topics covered, all three strategies, with differences in emphasis, touch on three elements of digital foreign policy that we outlined in our initial typology. Regarding digital topics, all strategies cover a wide variety of topics (see table two). Through a quantitative overview, we can detect small differences in emphasis. For example, Australia puts considerable emphasis on security. Data and privacy are the most mentioned topics in the Swiss, Dutch, and French strategies. Overall, the Swiss strategy offers the most balanced approach. We can see that digital development, with a focus on access to networks, is present in all the strategies. Human rights are most often mentioned in connection with protection of privacy and freedom of expression. When it comes to the economy, e-commerce, the free flow of data, and competition policies are key issues. In terms of security, emphasis is placed on the protection of critical infrastructure and the fight against cybercrime. We can also see that ‘states are increasingly defining their positions on how international law applies to cyberspace in regard to cyber conflicts, and are additionally preparing for greater regional and international cooperation related to international peace and cybersecurity’ (Kurbalija & Höne, 2021)

Table 2: Coverage of specific issues based on the frequency of certain terms

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of total words</td>
<td>23,213</td>
<td>4,051</td>
<td>23,285</td>
<td>10,753</td>
<td>18,177</td>
</tr>
<tr>
<td>data &amp; privacy</td>
<td>27</td>
<td>7</td>
<td>135</td>
<td>98</td>
<td>76</td>
</tr>
<tr>
<td>AI/artificial</td>
<td>22</td>
<td>1</td>
<td>5</td>
<td>19</td>
<td>8</td>
</tr>
<tr>
<td>security</td>
<td>165</td>
<td>13</td>
<td>45</td>
<td>25</td>
<td>58</td>
</tr>
<tr>
<td>human rights</td>
<td>75</td>
<td>9</td>
<td>39</td>
<td>16</td>
<td>30</td>
</tr>
<tr>
<td>governance</td>
<td>32</td>
<td>3</td>
<td>60</td>
<td>1</td>
<td>26</td>
</tr>
<tr>
<td>development</td>
<td>17</td>
<td>31</td>
<td>94</td>
<td>71</td>
<td>74</td>
</tr>
<tr>
<td>science</td>
<td>9</td>
<td>0</td>
<td>28</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>economy/economic</td>
<td>82</td>
<td>3</td>
<td>68</td>
<td>47</td>
<td>59</td>
</tr>
<tr>
<td>cooperation</td>
<td>62</td>
<td>16</td>
<td>57</td>
<td>41</td>
<td>25</td>
</tr>
</tbody>
</table>
Third, the strategies emphasise both competition and cooperation and advocate for navigating a path between these two poles. All strategies are, to varying degrees, driven by self-interest. For example, the French strategy aims to ‘strengthen the influence, attractiveness and security of France and French digital players’ (Ministère de l’Europe et des Affaires étrangères, 2019). As mentioned above, the Swiss strategy aims to ‘raise Switzerland’s profile in the area of digital governance’ (FDFA, 2021). All strategies also raise concerns about increasing geopolitical competition. The Swiss strategy mentions increasing fragmentation ‘geopolitical renaissance is also evident in the digital space’ (FDFA, 2020, p. 6) The Australian strategy recognises that ‘competition over technology is increasingly at the centre of international politics and foreign policy’ (Australian Government, 2021, p. 7). In the Danish strategy, there is an explicit mention of ‘the strategic competition between the US and China’ (Ministry of Foreign Affairs of Denmark, 2021, p. 4). On the side of cooperation, all strategies make reference to relevant multilateral (global and regional) fora and emphasize the need for cooperation. France for example strongly emphasises the role of the European Union and a European approach. Australia highlights the importance of cooperation in the Pacific (including capacity development) and alliances such as the Quad Tech Network (consisting of Australia, Japan, India, and the USA).

Fourth, capacity development is explicitly mentioned in four strategies. This concerns building international capacities in relevant ministries and agencies and supporting the development of capacities of other countries and stakeholders to meaningfully participate in global debates. For simplicity of discussion we will call the former internal capacity building and the latter capacity development in the context of cooperation and development. The French strategy focuses on capacity development in the context of cooperation and development (Development and Digital Plan), which includes support in the areas of infrastructure, services, regulation, and governance. The Dutch strategy places great emphasis on capacity development in the context of cooperation and development. Internal capacities are mentioned in the context of needing to recruit staff with relevant expertise. Switzerland discusses capacity development in relation to supporting developing countries and focuses on digital technologies and cybersecurity and aims to support ‘both the ability to develop strategies and policies as well as specific technical expertise’ (FDFA (b), 2021, p. 9). Since the release of its initial strategy in 2017, Australia has placed
explicit emphasis in training diplomats and staff from other ministries in digital diplomacy and digital foreign policy (Cyber Affairs Curriculum of the Diplomatic Academy). The Australian strategy mentions external capacity building in a number of policy contexts, including cybersecurity and cybercrime, international law, democratic principles, and human rights. Areas of focus and engagement are ASEAN and the Pacific.

Fifth, the shifts brought about by digitalisation and the diplomatic and foreign policy responses also need to be reflected in institutional and organisational terms. All five countries have created dedicated ambassadorial positions, which typically serve as representatives towards other states, the tech industry, and other stakeholders. They also have an internal coordination role. This is explicitly discussed in the Australian strategy and its International Cyber and Critical Technology Engagement Group (Australian Government, 2021, p. 14) can serve as an illustrative example. This group brings together five different ministries, the prime minister’s office, the attorney-general’s office, federal police, and the cyber security centre. It is coordinated by the Ambassador for Cyber Affairs and Critical Technology.

3. Recommendations for practising digital foreign policy

It is clear that ‘digital’ has become an important aspect of foreign policy. In the previous sections, we focused on outlining the key elements of digital foreign policy and highlighting the approach taken in five comprehensive digital foreign policies.

What approach countries take will depend on their specific context and the available capacities. When it comes to the practise of digital foreign policy, there are, however, three general shifts that need to be taken into account. First, there are new actors on the diplomatic playing field. Second, old and new venues need to be taken into account. Third, diplomatic practice needs to navigate a mix of tradition and innovation by paying attention to the 4 ‘multi’-approaches. These three shifts are interconnected and interdependent. Let us look at three shifts in more detail.
First, the practice of digital diplomacy needs to recognise that there is a wide range of actors that need to be taken into account. These actors reflect digital power (e.g. the tech industry), developing networks (e.g. academia and research), and concern for public interest and human rights (e.g. civil society). The strategies we have analysed in the previous section highlight multistakeholder governance and the need to engage all relevant actors both at the international and the domestic level.

In particular, the power of tech companies and the need to involve them in the governance of the digital space needs to be recognised. They, for example, play a critical role in running digital infrastructure. They also represent veritable economic power. The market capitalisation of Apple, for example, reached US$2.5 trillion in October 2021 (Statista, 2021a). In comparison, the total GDP of Latin America and the Caribbean was US$4.7 trillion in 2020 (World Bank, 2021). Furthermore, this economic power is linked to the ‘social power’ of tech companies. Companies like Meta (Facebook) with its almost 3 billion users (Statista, 2021b), have insights into social dynamics and take decisions that can shape these dynamics. Governments are aware of these shifts in power and some have started engaging the tech industry through diplomatic efforts, including but not limited to the appointment of tech ambassadors (Horejsova et al., 2018). Tech companies themselves have started to shift from lobbying to more long-term engagement and participation in diplomacy. For example, Microsoft opened a representative office at the UN in New York (Franck, 2020).

The second shift requires the recognition of both traditional and new venues for diplomatic practice. Traditional diplomatic venues are for example the multilateral hubs in New York and Geneva. In terms of digital topics, Geneva plays a particularly important role. Most practical and functional aspects of digitalisation are negotiated and implemented via Geneva-based organisations, from telecommunications (ITU), to standardisation (ISO, IEC, ITU) and e-commerce (WTO), to name a few. In addition, new venues around the fast-growing tech industry have emerged. These include the San Francisco Bay Area, Shenzhen, Bangalore, and the ‘Silicon Savannah’, near Kenya’s capital Nairobi. Looking in more detail at the Bay Area, various forms of diplomatic representation can be identified, including tech ambassadors and their offices, consulates general, innovation centres, investment promotion agencies, and honorary consuls (Horejsova et al., 2018, p. 4).

Building on these two observations, it is clear that diplomats need to mix tradition and innovation in their approach. This is the third shift we have identified and it is best encompassed by the 4 ‘multi’-‘approaches: multilateral, multi stakeholder, multidisciplinary, and multilevel approaches.
• Multilateral diplomacy plays an important role in addressing digital issues. It is clear that most concerns cannot be addressed by governments in isolation. The global nature of the internet requires global solutions. The World Summits on Information Society (WSIS) in 2003 and 2005 and the UN Government Group of Experts on Cybersecurity (UN GGE), which held its first meeting back in 2004, are two examples from the early days of digital governance. As mentioned above, multilateral hubs such as Geneva have become important venues for addressing a wide variety of digital issues.

• Multi Stakeholder approaches take into account that a variety of actors are relevant in addressing particular issues. As we have seen above, this is nowhere more true than in addressing digital topics. The multistakeholder approach is closely associated with digital topics since the World Summits on the Information Society (2003 and 2005). The Internet Governance Forum (IGF) is a particular example of multi stakeholder approaches.

• A multidisciplinary approach reflects the cross-cutting nature of digital issues, particularly its technical, economic, legal, social, and human rights aspects. Traditional policymaking is typically contained in silos, which commonly use a specific language, and frame issues in particular ways. For effective digital governance, these silos need to be overcome or, at the very least, effectively bridged.

• Multilevel governance addresses policy issues as close as possible to those affected by the policy in question. The Internet is global in operation but its effects are felt nationally and locally. Good digital foreign policy takes this into account. For example, the Swiss comprehensive digital foreign policy strategy follows this multi-level approach by building on the subsidiarity principle inherent in the Swiss political system.

4. Conclusions

In this article we offered a definition and typology of digital foreign policy. We argued that digital foreign policy is emerging and that countries need to actively shape it in order to ensure future prosperity. We described digital foreign policy as the realisation that all aspects of diplomacy and foreign policy are impacted by digitalisation and its consequences and
that a comprehensive and coordinated approach is needed in the face of accelerated digitalisation processes and their impacts. We argued that ‘digital’ can be understood as (a) new topics on diplomatic agendas, (b) new tools, and (c) a changed environment in which diplomacy is practised.

We analysed five comprehensive digital foreign policy strategies and highlighted similarities and differences in approach. In particular, the differences in terminology are noteworthy. We also noted that these strategies (a) cover a broad range of similar topics but do show diversity in their particular emphasis, (b) navigate a space between international competition and international cooperation, (c) address capacity development needs, and (d) touch on aspects of coordination, institution-building, and personnel. We then highlighted three shifts in practice that need to take place in order to foster effective digital foreign policy: (a) engaging new actors on the diplomatic playing field, (b) being active on old and new venues of diplomacy, and (c) navigating foreign policy and diplomacy between tradition and innovation.

From this analysis it becomes clear that in order to engage effectively in digital foreign policy, a re-organisation of ministries of foreign affairs is necessary. Newly created positions and units need to reflect digital foreign policy goals. Individual training and capacity development also need to take these shifts into account. Given the broad range of topics and the number of domestic actors that need to be involved to address these topics, a whole-of-government and whole-of-society approach are useful tools for effective digital foreign policy. In small and developing countries in particular, businesses, academia, civil society, and other national actors can be engaged in creating and implementing digital foreign policies. This could be the only way to establish and maintain representation in the highly-diversified and complex field of digital governance.

REFERENCES


