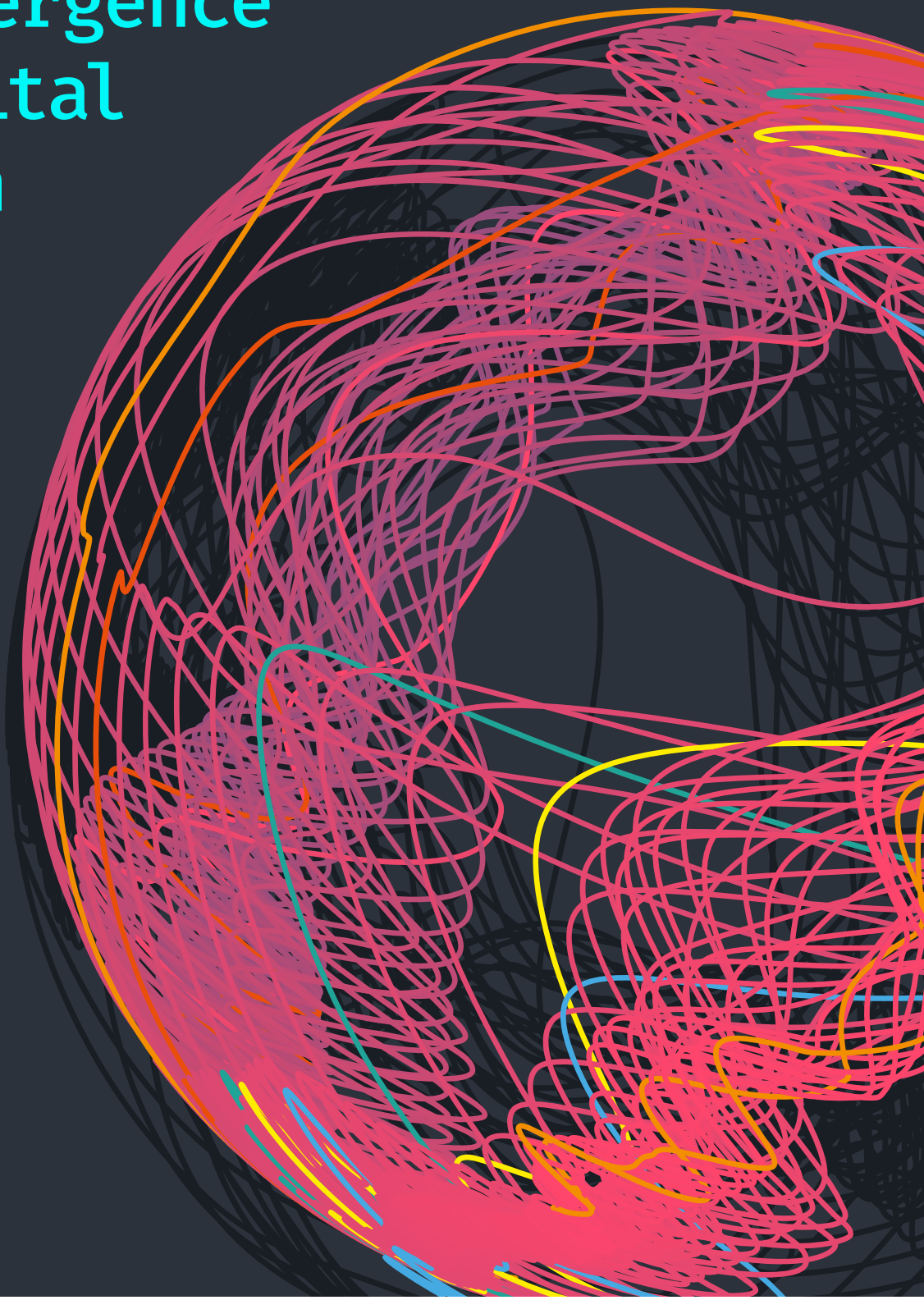
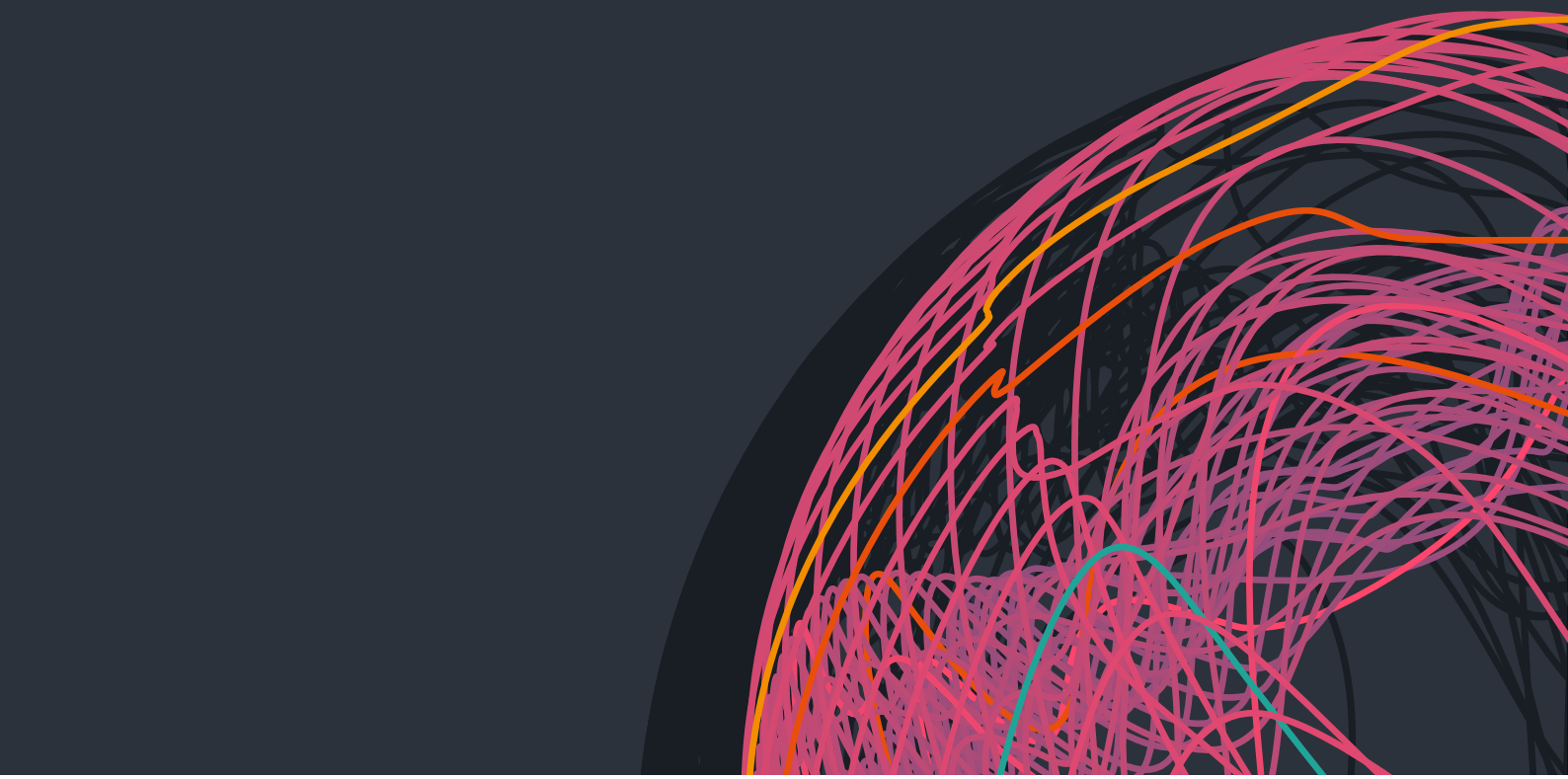
2021: The emergence of digital foreign policy



Jovan Kurbalija
Katharina Höne

DiPLO
Geneva Internet Platform



Impressum

Author: Jovan Kurbalija, Katharina Höne
Research support: Katarina Anđelković, Nataša Perućica
Layout and design: Viktor Mijatović
Copy-editing: Maja Bačlić

Malta
DiploFoundation Anutruf, Ground Floor Hriereb Street, Msida MSD 1675 Malta

Switzerland
WMO Building (2nd floor) 7bis, Avenue de la Paix CH-1202 Geneva, Switzerland

Publication date: March 2021
For further information, contact DiploFoundation at diplo@diplomacy.edu

To download an electronic copy of this report,
visit www.diplomacy.edu/digitalforeignpolicy_paper_March2021

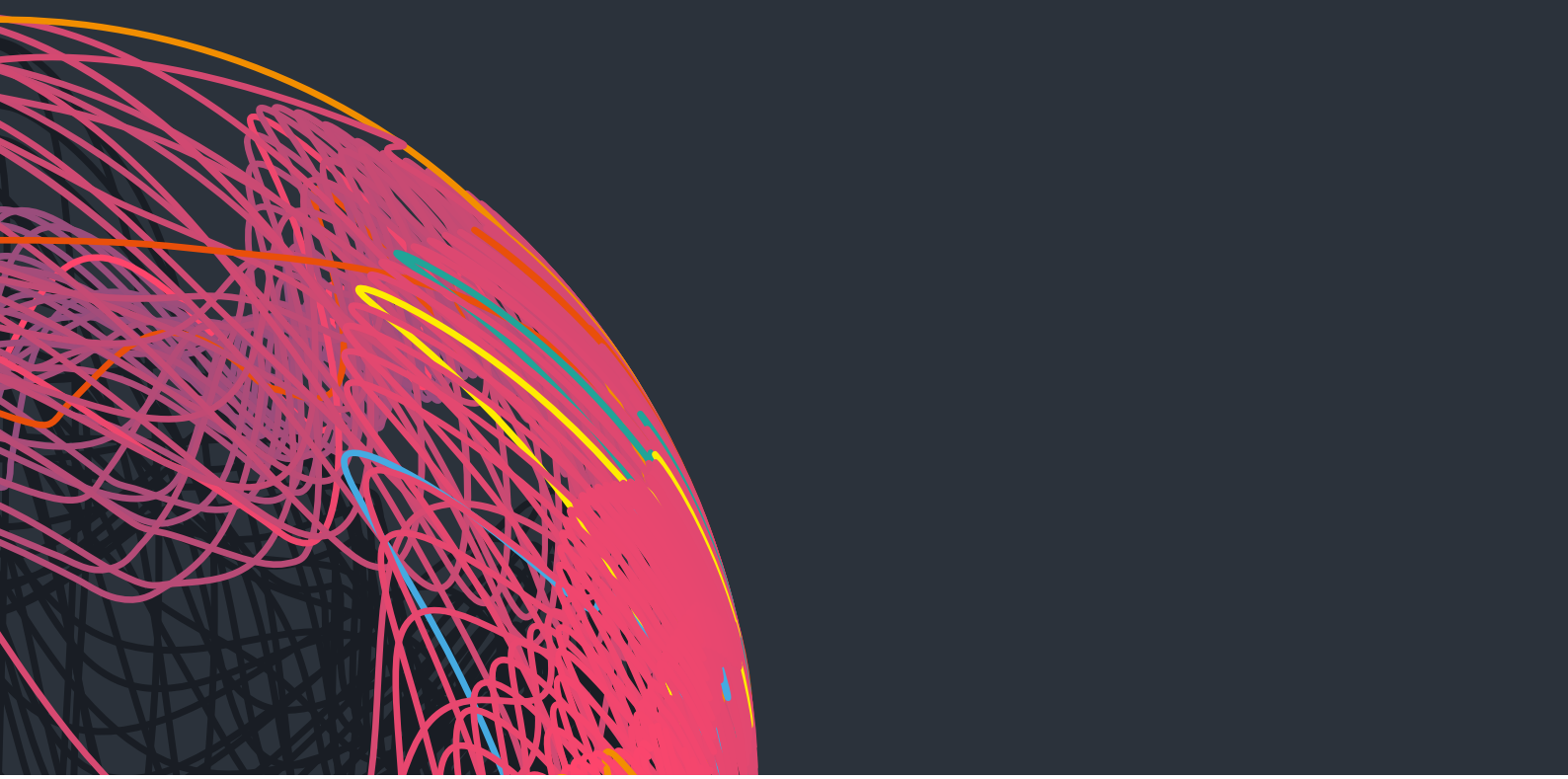


Table of contents

Introduction

In November 2020, Switzerland introduced its Digital Foreign Policy Strategy, marking a new phase in its commitment to digital foreign policy and the governance of digital issues. For decades, Switzerland has been at the forefront of international digital developments. It hosted the World Summit on Information Society (WSIS) in Geneva in 2003, and played an instrumental role in launching the Internet Governance Forum (IGF). It additionally pioneered the Organization for Security and Co-operation in Europe's (OSCE) confidence-building measures back in 2013. Currently, Switzerland chairs the UN Open-Ended Working Group on Cybersecurity (OEWG). Together with other countries, such as Singapore, Estonia, and the Netherlands to name a few, it has been among the most prominent contributors towards a more inclusive and impactful digital governance globally.

As many countries worldwide look for ways to deal with the digitalisation of foreign policy, the Swiss strategy can serve as a very useful guideline. It brings terminological and conceptual clarity in addressing the interplay between **digital and diplomacy**.

The Head of the Swiss Federal Department of Foreign Affairs, Ignazio Cassis, argued that 'digitalisation is on the one hand an instrument, helping to simplify processes, for example in the area of consular services or IT. On the other, it is also a foreign policy matter.'

This distinction is echoed in Diplo's research and teaching methodology, which focuses on three main areas of digitalisation's impacts on diplomacy:

- Changes in the political, social, and economic **ENVIRONMENT** in which diplomacy is conducted (e.g. the nature and distribution of power, new types of conflicts, and the changing nature of sovereignty and interdependence in international relations)
- The emergence of new policy **ISSUES** in foreign policy such as cybersecurity, privacy, data governance, e-commerce, and cybercrime
- The use of digital **TOOLS** in the practice of diplomacy such as social media, online conferencing, and big data analysis

While digital tools, in particular social media, have been gradually introduced to the practice of diplomacy, many open questions remain regarding the impact of digitisation on foreign policy and the environment in which diplomacy is practised. This is where digital foreign policy becomes important.
This paper uses **five main questions** to reflect on digital foreign policy:

- Why? Promoting national interests in the era of digital interdependence
- What? Key digital policy issues
- Who? Governments, tech companies, and civil society
- Where? Multilateral and new business policy venues
- How? A mix of tradition and innovation in diplomatic practice

Join the conversation!

You can follow Diplo's ongoing research on digital foreign policy here. The page includes a mapping of the main policy approaches as well as summaries of selected digital foreign policy strategies (Australia, Denmark, France, the Netherlands, Norway, and Switzerland).

WHY?

Promoting national interests in the era of digital interdependence

The **protection and promotion of national interests** – the core function of diplomatic services – is being increasingly shaped by digitalisation. For example: cybersecurity impacts national security; online platforms support the economic well-being of citizens and companies; the internet facilitates health, education, and other critical services for society, especially during crisis as it has been doing during COVID-19 and other pandemics.

While societies become digitally dependent, governments, with the exception of China and the USA, have very few policy and legal tools to protect the interests of their citizens and companies online. Most governments can do very little if, for example, the data of their citizens is not protected or if their companies are removed from an online platform.The data firm Cambridge Analytica is a good case in point. The more recent move of Australia to protect the business interests of its media outlets vis-a-vis Facebook and Google is another.

For these and many other policy challenges, governments and their diplomats must develop international mechanisms for protecting online rights and the interests of their citizens and companies. Ultimately, these solutions will boil down to answering the question 'whom to call' to address digital policy issues

Figure 1 'Whom to call' on digital issues.

International policy solutions must be found through the **management of digital interdependence** which has increased considerably over the past years, and especially during the pandemic. Zoom meetings, ordering meals via UberEats, following courses on Moodle, and many other (now critical) services depend on a complex infrastructure that criss-crosses national borders. Digital interdependence triggers new vulnerabilities and increases risks. These risks become obvious when national leaders ask a simple question: What could happen if their country disconnects from the internet for any amount of time? Answer: The daily lives of millions would be seriously affected across the board, from communicating with family and friends, to having access to their jobs and critical services. Containing the growing risks and harnessing the benefits of digital interdependence are quickly becoming key diplomatic tasks.

The **digitalisation of traditional policy issues**, such as trade, health, and the environment, is another major challenge for diplomatic services. E-commerce is taking up more and more of the World Trade Organization's (WTO) bandwidth. Data, artificial intelligence (AI), and infodemics now feature far more prominently on the agenda of the World Health Organization (WHO). Climate change debates are increasingly linked to digitalisation and the circular economy. Additionally, mediators in conflicts worldwide are using social media and other digital tools that impact internal conflicts.

Diplomats have to transform traditional policy spaces, approaches, and procedures in order to deal with the impacts of digitalisation. By promoting national interests online, managing digital interdependence, and transforming the traditional policy agenda, diplomatic services across the world can reform their modus operandi and contribute to the building of a 'digital home for humanity' that would serve as a space where digital policy issues can be addressed in inclusive, informed, and impactful ways.

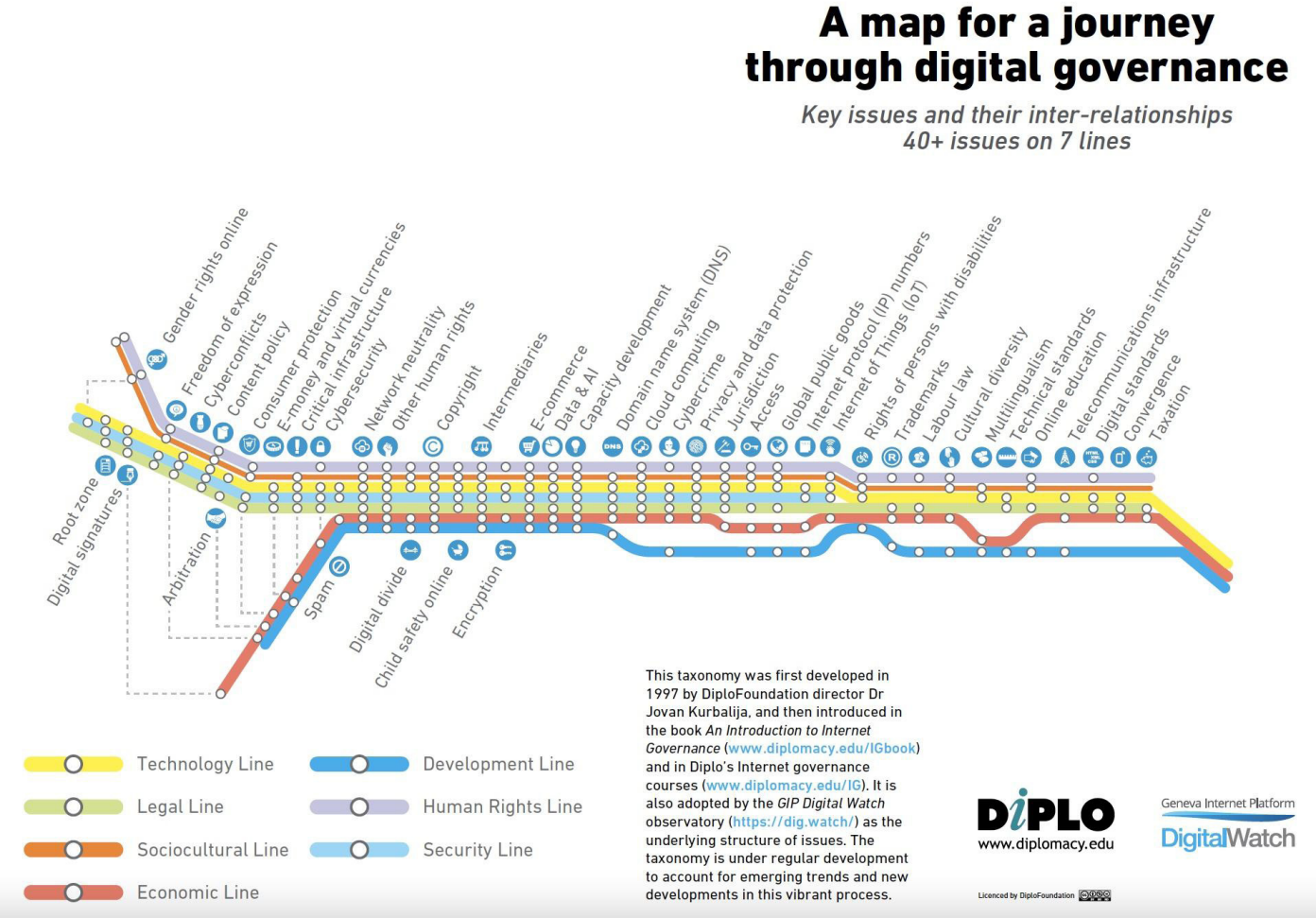


Figure 2 A map for a journey through digital governance (DiploFoundation and the Geneva Internet Platform).

WHAT?

Key digital policy issues

Diplo's **digital policy taxonomy** includes more than 50 digital policy issues. In this taxonomy, issues are organised in seven baskets: Technology, Security, Human rights, Economy, Development, Legal, and Sociocultural. In Figure 2, each basket is presented as one subway line, while the issues are displayed as stops. The map also illustrates the various interplays between baskets and issues.

So far, the following issues have dominated most of the global digital policy agenda:

- Internet infrastructure centred around global connectivity standards and strategies, addressed through the International Telecommunications Unions (ITU) and the management of internet names and numbers in the context of the Internet Corporation for Assigned Names and Numbers (ICANN)
- E-commerce policymaking in the WTO
- Cybersecurity at the UN and at regional organisations
- Protection of privacy and freedom of expression at the United Nations Human Rights Council (UNHRC)

Over the past two years, digital policy has been moving beyond these issues towards dealing with a wide range of foreign policy issues. This shift is clearly signalled by the UN Secretary General's Roadmap for Digital Cooperation which includes more than 30 digital policy issues ranging from digital inclusion to cybersecurity, AI, and digital governance.

National approaches to digital foreign policy have been emerging from the bottom up, focusing mainly on either infrastructure (ITU deliberations and the 'ICANN agenda'), cybersecurity, e-commerce, or human rights. The easiest way to detect national focus is through the language used by governments. For example, 'digital' indicates a holistic approach, 'cyber' signals security, while 'tech' is more business-oriented. 'Online' has been used for human rights, and more recently during the pandemic, for describing online learning and meetings. The use of prefixes is also a matter of policy fashions and trends. Back in 2017, when Australia drafted its national digital strategy, 'cyber' was very popular and extended beyond issues of security to other fields. 'Tech' had a big uptake in Denmark after the term 'techplomacy' was coined. 'Digital-', as a prefix, has been the most robust and precise prefix used in describing new phenomena. Table 1 shows a survey of prefixes used in five digital foreign policy strategies. Switzerland, France, and the Netherlands signal a more holistic approach, while Australia seems to focus more on the cybersecurity angle of digital issues.

Table 1 The use of prefixes in digital foreign policy strategies

	Denmark (2021)	Switzerland (2020)	Netherlands (2019)	Australia (2017)	France (2017)
No. of total words	4,051	23,285	10,753	23,466	18,177
cyber	13	66	25	755	89
online	1	16	28	122	12
digital	37	312	209	211	223
virtual	0	6	0	1	1
net	0	1	0	4	0
tech	77	4	2	0	0
e	0	1	2	0	2

A few common **policy issues** appear among these national strategies:

- Digital development, with a focus on access to networks, features in all the strategies. They differ in linkages to the 2030 Agenda and the achievement of the sustainable development goals (SDGs) by emphasising issues such as capacity development, health, and digital.
- Human rights coverage is typically centred around the protection of privacy and freedom of expression as these issues are most directly affected by digitalisation. In most cases, a more holistic approach to human rights online is yet to be developed.
- Economic aspects are centred around digital economy: e-commerce, the free flow of data, and competition policy.
- Security issues mainly focus around the protection of critical infrastructure and the fight against cybercrime. 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.

Table 2 shows the coverage of specific issues by tabulating the frequency of certain terms.

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

	Denmark (2021)	Switzerland (2020)	Netherlands (2019)	Australia (2017)	France (2017)
No. of total words	4,051	23,285	10,753	23,466	18,177
data & privacy	7	135	98	19	76
AI/artificial intelligence	1	53	19	0	8
security	13	45	25	217	58
human rights	9	39	16	83	30
governance	3	60	1	67	26
development	31	94	71	93	74
science	0	28	2	4	3
economy/economic	3	68	47	69	59
cooperation	16	57	41	72	25
research/education	5	40	24	22	24
health(care)	3	16	11	5	2
sustainable development goals (SDGs)	0	6	5	1	2

While word choice reflects particular focuses, national strategies also demonstrate countries' foreign policy priorities and their levels of digital developments.

Denmark (2021): The Danish strategy centres around three pillars: responsibility, democracy, and security. While other strategies barely use 'tech' as a prefix, it is by far the most referred to prefix in the Danish strategy. The strategy uses the term 'development' greatly, however, it makes no direct mention of sustainable development goals (SDGs).

Switzerland (2020): The Swiss strategy is the most comprehensive strategy covering more than 30 issues (as per Diplo's taxonomy) and organised in 4 main baskets: digital governance, prosperity and sustainable development, cybersecurity, and digital self-development.

Compared to other strategies, the Swiss strategy has the following unique features:

- Using data as the cross-cutting aspect of the strategy. 'Data' was mentioned 125 times, referring to the following 7 baskets: Technology (standardisation, interoperability, the cloud, links to AI), Human rights (privacy protection, personal data ownership), Economy (commodity, digital trade competition), Security (dependence, conflict resolution, humanitarian assistance), Legal (jurisdiction, intellectual property rights (IPRs)), Development (humanitarian assistance, sharing, fairness, global public goods, sustainable development, health, climate change, electronic waste), and Sociocultural (sharing, fairness).
- The concept of digital self-determination anchors digital policy in the core values of humanity, including through the protection of privacy, freedom of choice, social benefits, and democracy. Individual self-determination is centered around control and the use of personal data, including the right to decide who can access such data.
- Science is highlighted as an inspiration and a driver of technological change. The Swiss strategy includes quite a few practical points on the links between science and diplomacy.

The Netherlands (2017): The Dutch strategy emphasises development, security, human rights and freedoms, and economy and trade. It is worth noting that the term 'digital security' appears in the document as a broader category (see section 'Digital security and freedom online'), covering the issues of cybersecurity, human rights, and the responsible use of data. 'Data' was also used greatly, mostly in reference to privacy, security, personal data protection, data flows, and localisation requirements.

Australia (2017): As illustrated in Figure 3, Australia has established a comprehensive approach from a cybersecurity angle. The policy areas the strategy covers include digital trade, cybercrime, international security, internet governance, human rights, and development, all of which are determined with cybersecurity firmly in mind.

Figure 3 Policy areas covered in Australia's digital foreign policy strategy (Australia's Cyber Engagement Strategy, p. 85).

The strategy does not feature data highly (only 13 references) and does not mention AI at all. It does establish a quarterly whole-of-government meeting convened by the ambassador for cyber affairs. In addition, there is an Industry Advisory Group for public–private engagement in the area of cybersecurity.

France (2017): The French strategy covers governance, economy, development, and security. It specifically promotes open and inclusive internet governance, calls for measures to build trust on the internet, and highlights an aim to promote the European digital model as a balance between multilateral and multistakeholder approaches. The implementation of the strategy is the responsibility of France's anointed tech ambassador. With the implementation of the strategy, France aims to become an important digital hub.

WHO?

Governments, tech companies, and civil society

Digital policy involves a wide range of actors which reflect: digital power (tech industry), developing networks (academia and research), and concern for public interest and human rights (civil society). Most digital foreign policy strategies express the need for multistakeholder governance as a way to engage all relevant actors on the national and international levels.

Tech companies are the main actors in this space, and this reflects their critical role in running digital infrastructure and their growing economic power. For example, Apple's market capitalisation at the end of 2020 (US$2.23 trillion) was similar to the total 2019 GDP of the entire African continent (US$2.33 trillion), and is close to the GDPs of the UK (US$2.81 trillion), France (US$2.79 trillion), and India (US$2.69 trillion). For a detailed comparison of the economic power of governments (GDP) and companies (revenue and market capitalisation), please consult Diplo's Data Engine.

Furthermore, Big Tech's economic power is intertwined with its 'social power', as tech platforms have deep insights about how society functions, from people's purchasing patterns and personal habits, to their political preferences.

Aware of this power shift, many governments have started engaging the tech industry by, for example, establishing a new kind of diplomatic representation in the Bay Area, Bangalore, and other centres of digital dynamism across the world (see section 'Where?').

As for tech companies, there has also been a noticeable shift from traditional corporate lobbying to more long-term participation in diplomacy. For example, Microsoft was among the first companies to pursue 'diplomacy' by establishing its presence in the main diplomatic centres, including the UN, and through an active participation in cybersecurity, development, and human rights initiatives.

Academia, the tech community, and civil society were dominant players in the early days of the internet when it was mostly being developed at universities and research centres. As the internet became more commercialised in the early 2000s, businesses became more involved in running the internet. This process has accelerated over the past decade with the fast growth of the digital economy. For example, digital standards were once an almost exclusive domain of tech and engineering communities. Lately, tech companies have been shaping standardisation initiatives. Academia, the tech community, and civil society have to strengthen their presence and influence in digital policymaking. In particular, as the 'third main actor' (next to governments and businesses), they should ensure the protection of public interests during negotiations on content policy, data protection, AI ethics, and other issues with a broader social impact. In addition, due to their vast global networks, they have the means for operational cooperation, and thus the power for implementing global policies. For example, the implementation of global cyber norms thanks to the international cooperation of various computer emergency response teams (CERTs) through their global Forum of Incident Response and Security Teams (FIRST).

WHERE?

Multilateral and new business policy venues

Traditional diplomatic venues are centred around New York City (the headquarters of the UN) and Geneva (the operational hub of the UN system). Geneva has a long tradition of governing the interplay between technology and diplomacy, dating back to the nineteenth century when the International Telecommunication Union (ITU) was established. Today, 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. Most countries have developed expertise and experience in following digital developments via their permanent missions in Geneva. The UN technology envoy, appointed by the UN secretary general, is a new actor who will play a vital role in the digital engagement of the UN system with governments, businesses, and other actors active in this field.

New digital policy centres have emerged around the fast-growing tech industry. In the USA, digital economic dynamism is based in the San Francisco Bay Area, which hosts most leading tech companies. As Diplo's study shows, more than 50 countries have been developing their representation in the Bay Area, either via traditional consulates in San Francisco or via new types of representation such as the Swissnex hub. While presence in the Bay Area is important for understanding what's coming next, and for attracting investment, tech companies, on the other hand, station most of their governance units in Washington DC or Boston, highlighting the growing interdependence between governments and Big Tech.

In China, most of the digital dynamism is happening in the Shenzhen area, while Beijing acts as the regulatory and policy centre for digital issues. Bangalore is India's technology hub, while 'Silicon Savannah', near Kenya's capital Nairobi, is one of Africa's IT hubs.

In Europe, Brussels is the regulatory capital and exudes global impact. Rules adopted in Brussels are often mimicked worldwide as has been the case with data regulations. The increasing ties between EU development aid and efforts related to digital, makes Brussels an important place for developing countries to establish a diplomatic presence. London is an important financial centre and a hub for AI developments. Paris is home to the Organisation for Economic Co-operation and Development (OECD), a place where taxation and other digital policies are discussed, as well as the United Nations Educational, Scientific and Cultural Organization (UNESCO), an organisation that plays an important role in AI governance. The International Organisation of the Francophonie (OIF) is also increasing its involvement in the digital realm. Vienna hosts the Organization for Security and Co-operation in Europe (OSCE) which does important work on cybercrime.

HOW?

A mix of tradition and innovation in diplomatic practice

The ways in which digital policy is developed builds on a mix of traditional and innovative diplomatic techniques. These techniques can be summarised in four 'multi-' categories: multilateral, multistakeholder, multidisciplinary, and multileveled.

MultiLATERAL digital governance has important centres in multilateral forums. The World Summit on Information Society (WSIS), which kicked off in Geneva (2003) and Tunis (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. Now the ITU, the WTO, and other international organisations (see section 'Where?') form important venues for discussing aspects of digital governance. A new phase has started with the digitalisation of specialised policy fields such as trade, human rights, and health.

MultiSTAKEHOLDER policymaking reflects the fact that most of the digital world is run by a wide range of private and non-state actors. For example, it is difficult to effectively regulate and manage e-commerce without the involvement of tech companies. The development of digital standards requires the involvement of academic, professional, and technical organisations. Multistakeholder processes require new skills and techniques, including effective communication among different professional cultures as illustrated below. Examples of multistakeholder venues or processes include the IGF, the Paris Call for Trust and Security in Cyberspace, and the Global Forum on Cyberexpertise (GFCE).

Figure 4 Speaking different languages.

In addition, we might see the development of a new 'hybrid' governance approach, The proposal of an IGF+ by the High-level Panel on Digital Cooperation is such a hybrid model. At ICANN, a multistakeholder space, there is the Government Advisory Committee which brings together national governments.

A **multiDISCIPLINARY** approach reflects the cross-cutting nature of digital issues, particularly among the 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. Siloed policy processes are often demonstrated in academic and research coverage. For example, similar issues regarding digital governance (e.g. encryption) are subject to studies by a wide range of research communities, from telecoms, trade, content, AI, and other perspectives. Finding a way to tie the work of these communities is a more difficult task. As such, dealing with multidisciplinary policy issues will be the main challenge for diplomatic services, as well as for governments and our societies as a whole.

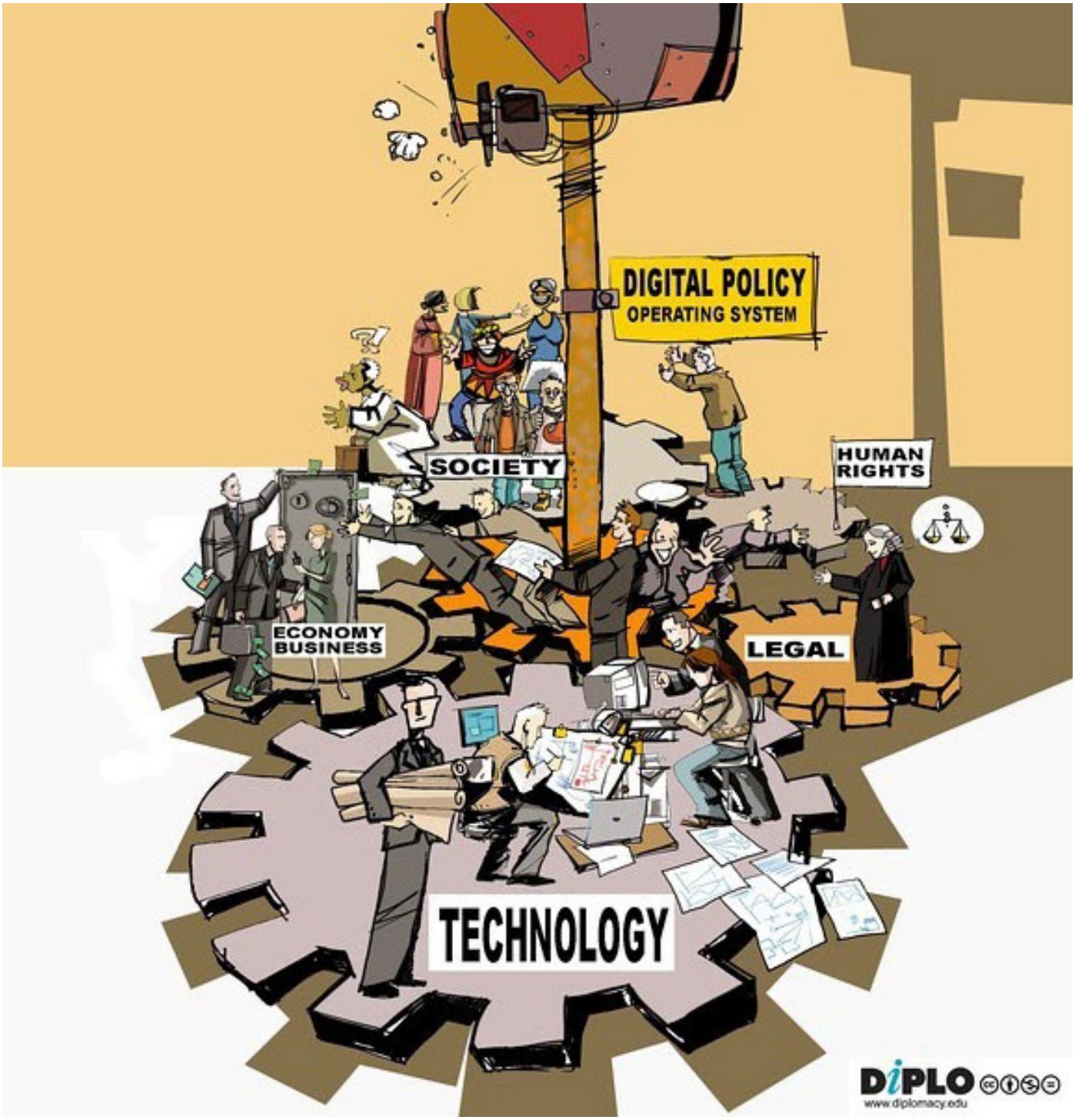


Figure 5 Digital policy operating system.

MultiLEVEL governance should address policy issues as close as possible to those affected by the policies in question. Such an approach also reflects the reality that, while the internet is global in its operations, its policy implications are often local and national. Switzerland's Digital Foreign Policy Strategy 2021–2024 follows a multilevel approach via the well-developed subsidiarity approach inherent in the Swiss political system. As Figure 6 shows, the main challenge is to ensure that 'policy elevators' move both ways (up and down) across local, national, regional, and global levels. Transparency and clarity in using a multilevel approach can prevent 'policy laundering', i.e. addressing the same issue on different policy levels.

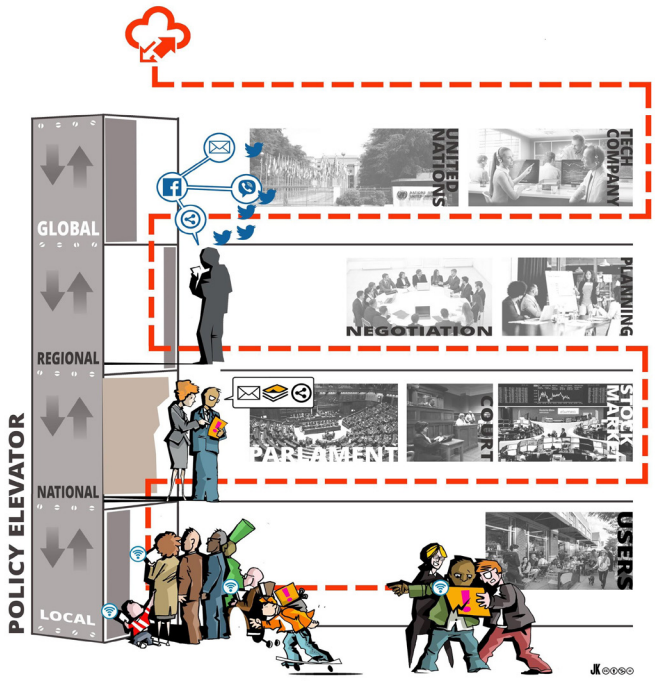


Figure 6 Policy elevator.

NEXT STEPS

Developing a digital foreign policy

Developing a digital foreign policy requires three main steps, starting with the reorganisation of diplomatic services as the basis for a whole-of-government and ultimately a whole-of-country approach.

Typically, the **reorganisation of diplomatic services** starts with the appointment of tech/digital/cyber ambassadors as many countries have done. Their main task is to add a digital layer to traditional foreign policies. Australia and France established such roles in their digital foreign policy strategies. Denmark has been innovated by establishing a tech ambassador in Silicon Valley who also carries out visits to other centres of digital dynamism such as China and India. This role is built around the concept of a 'rowing ambassador'. Switzerland has chosen a gradual and decentralised approach which reflects the country's political culture. Tech and security ministries have developed their own diplomatic capacities and represent Switzerland in specialised negotiations. Switzerland's Digital Foreign Policy Strategy is a careful balancing act between providing the necessary coordination among different actors while avoiding unnecessary centralisation. As Switzerland is upgrading its foreign policy structure, it will be interesting to follow how it will coordinate diplomatic activities regarding data, the central pillar of the Swiss strategy and an area which requires a cross-cutting approach which involves security, human rights, technological, economic, and other policy aspects.

India has established the New Emerging and Strategic Technologies (NEST) department which aims to coordinate its national policies and positions in international negotiations, from e-commerce to human rights and cybersecurity.

As countries develop organisational support, they also need to nurture the next generation of diplomats who should be skillful 'boundary spanners' that can engage people and institutions across professional and institutional delimitations. Recruitment and training should focus on a good mix of personal skills (such as empathy and active listening), as well as knowledge of a wide range of scientific, economic, and academic disciplines.

The next layer in creating an effective digital policy is a **whole-of-government approach**, involving a range of ministries and governmental departments. Tech ministries and regulators deal with policy and standards for technical infrastructure and critical internet resources (i.e. domain name systems, internet protocol numbers, etc.).

Economic and trade ministries focus on e-commerce negotiations through the WTO and regional trade agreements. Their main challenge is the introduction of non-trade issues such as cybersecurity and privacy policy into trade agreements.

Foreign affairs and security ministries have played a key role in cybersecurity negotiations at the UN level and in regional organisations. International legal experts of diplomatic services were particularly present in the UN GGE negotiations. Since the effects of cyberattacks can impact everything (from schools and financial services to state secrets and water supplies), various line ministries and public institutions need to be kept in the loop as well.

As digitalisation extends to other policy areas, specialised ministries are developing their own coverage in the fields of heath, migration, climate change, and others.

The main challenge for the whole-of-government approach is the coordination of foreign policy around highly cross-cutting issues such as AI and data governance.

The **whole-of-country or whole-of-society approach** is an umbrella for digital foreign policy topics. Many non-state actors already participate in international multistakeholder processes or have an interest in joining them. They can be important contributors to national efforts to cover a wide spectrum of more than 1,000 digital policy processes and initiatives worldwide. Even major actors such as the USA, the EU, and China, find it challenging to substantively follow all digital policy processes. The situation is much more severe with small

and developing countries which are increasingly absent from global digital negotiations due to limited capacities. Thus, engaging businesses, academia, civil society, and other national actors in creating and implementing digital foreign policies could be the only way to establish and maintain representation in the highly-diversified and complex field of digital governance.

Some embryonic forms of the whole-of-country approach have been emerging around the more than 100 national, regional, and local Internet Governance Forums which gather all national actors to discuss digital policies. The need for policy inclusion will require innovative approaches. For example, it will be interesting to follow how Switzerland will use direct democratic instruments for its whole-of-country approach as it was indicated in the Swiss strategy.

In the coming years, we can expect the development of new approaches and mechanisms for engaging a wide range of societal actors, which will further reflect the impacts digital developments have on all parts of our modern society.

Additional resources

In addition to this text, a few resources could help in developing a deeper understanding of digital foreign policy:

- Earlier research on the Swiss approach to internet governance can be found in Politorbis: Switzerland and Internet governance (No. 57, February 2014).
- For cybersecurity issues, consult the Swiss Cybersecurity Capacity Review.
- A wider framework of internet and digital governance can be found in An Introduction to Internet Governance.
- A detailed mapping of the Geneva digital scene is available via the Geneva Digital Atlas.

About DiploFoundation

DiploFoundation is as Swiss–Maltese non-governmental organisation that specialises in capacity development, particularly in the field of internet governance and digital policy.

Established in 2002, Diplo, among other things, works to improve the role of small and developing states in global diplomacy by:

- Training officials through online courses, workshops, and simulation exercises
- Developing capacities on internet governance, data, artificial intelligence, and other emerging tech issues
- Promoting and developing digital tools for inclusive and impactful governance and policy making

Over the years, Diplo has successfully trained over 6,400 alumni from over 200 countries and territories, including individuals working in governments, the private and civil sector, media, and academia.

About the Geneva Internet Platform

Since 2014, Diplo has been operating the Geneva Internet Platform (GIP) which provides a neutral and inclusive space for digital policy debates, digital policy monitoring and analysis, and capacity development. Its activities are implemented through just-in-time briefings and events, policy research, and the *GIP Digital Watch* online observatory which serves as a comprehensive one-stop shop for the latest digital policy developments, overviews, trends, events, actors, instruments, and other resources.