Coronavirus: the role of digital tech & policy

TRENDS IN FEBRUARY
Developments in EU digital policy, the interplay between health and digital technologies, and international discussions on cybersecurity

FROM THE OBSERVATORY
The month’s top digital issues: security, human rights, jurisdiction, new technologies, and the Internet economy

IN FOCUS
Points of convergence and divergence in OEWG discussions of responsible state behaviour in cyberspace

IN FOCUS
Trust and excellence: European Commission ambitions in AI and the data economy
The top digital policy trends in February

Each month we analyse hundreds of unfolding developments to identify key trends in digital policy and the issues underlying them. These were the trends we observed in February.

1. Shaping Europe’s digital future: European Commission plans

‘A Europe fit for the digital age’ is one of the six priorities of the European Commission’s 2019–2024 mandate. As the Commission recognises, this will involve ‘empower[ing] people with a new generation of technologies’ and ensuring that the EU leads the transition to a new digital world.

In February, the Commission presented three policy documents outlining objectives and plans regarding this priority: a Communication on Shaping Europe’s Digital Future, a White Paper on Artificial Intelligence (AI), and a European Strategy for Data.

The need to achieve European technological sovereignty reverberates across these documents. In the words of president Ursula von der Leyen, the goal is an EU that can ‘make its own choices, based on its own values, respecting its own rules’. Such an EU would be less dependent on non-European infrastructures and technologies, and could ‘act as one and define its own way in the digital economy’. Beyond technological sovereignty, the Commission wants the EU to become a trusted digital leader, with a competitive digital economy that reflects not only a strong industry but also a focus on European values and fundamental human rights.

The Commission identifies three policy priorities central to achieving these high-level objectives: supporting the development, deployment, and use of technologies that work for people; building a fair and competitive digital economy; and promoting an open, democratic, and sustainable digital society. The AI white paper’s primary focus is on exploring governance and regulatory approaches to ensure the trustworthy and secure development and uptake of AI. While asserting that several EU rules and regulations are already relevant to AI (although some may require adjustments), it also proposes the development of a new regulatory framework for high-risk AI applications. The data strategy, lastly, is geared towards securing a leading role in the global data economy for the EU, and proposes policy and regulatory measures that could lead to the creation of a single European data space. Read more on pages 8–9.

Both the AI white paper and the data strategy are under public consultation. This is an interesting development, since von der Leyen’s initial plan was to propose AI legislation in the first 100 days of the mandate; instead, the Commission has chosen to present several governance and legislative options and invite feedback from stakeholders before taking further steps. This will have benefits for inclusiveness, but a potential concern is that the public consultation and follow-up processes may be lengthy; with the rapid pace of developments in tech, especially in AI, it is unclear that the EU can afford delays in strengthening its policy and regulatory approaches.

2. The interplay between health and digital technologies in focus

The coronavirus (COVID-19) outbreak brought into sharper focus the close interplay between the digital and health sectors. Digital technologies have been crucial in efforts to control the spread of the virus, with measures including mobile apps enabling people to assess if they are at risk of contracting the virus and AI-powered temperature screening tools deployed in public spaces in China and elsewhere.

Efforts have also been made to address the spread of misinformation related to the virus online and to help authorities and experts share reliable information. Uber and Airbnb have suspended activities in certain regions and several major tech events have been canceled due to coronavirus concerns, including the World Mobile Congress in Barcelona and the Internet Corporation for Assigned Names and Numbers (ICANN) meeting in Cancun (which is now planned to be held fully online). Read more on page 6.

Coronavirus is a public-health emergency, but many other developments in digital health are ongoing over the longer term. The applications of AI, for instance, range from surgical robots to algorithms that improve medical diagnostics to machine learning techniques that aid in the research and development of new medicines. That there has been continuing progress in these areas is shown by two studies published in February: One found that AI outperformed...
Digital Watch Newsletter

3. Cybersecurity: in search of a breakthrough in international cooperation

Cybersecurity was high on the international agenda in February. The Munich Security Conference – a high-level conference focused on international security – dedicated one session to cybersecurity, but other discussions also touched on digital technologies and their implications for national and international security. This is a clear sign that cybersecurity is becoming a topic of mainstream and high-level concern, given its implications across a wide range of areas, including national security, global peace and stability, international cooperation and partnerships, and economic and trade policy.

Ongoing tensions between the USA and China over tech issues, and their security dimensions in particular, were evident in Munich. US Secretary of State Michael R. Pompeo described ‘Huawei and other Chinese state-backed tech companies [as] Trojan horses for Chinese intelligence’ and US Secretary of Defense Mark Esper encouraged US allies to limit their reliance on Chinese 5G vendors to avoid rendering ‘critical systems vulnerable to disruption, manipulation, and espionage’, and to develop alternative 5G solutions themselves. However, China’s Foreign Affairs Minister Wang Wi rejected US criticisms as ‘lies’ and noted that his country was ready to engage in serious dialogue with the USA.

The conference also saw discussions of cooperation in the field of cybersecurity, with one notable test-case being recent collaborations between Germany and Singapore’s defence ministries. Governmental officials and representatives of large tech companies engaged in discussions on online misinformation, AI, and the politics of big data.

Debates over rules, norms, and principles for responsible state behaviour in cyberspace continued within the framework of the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), with both groups holding their second sessions in February. The OEWG discussions revealed that countries remain divided on key questions including whether existing norms are sufficient for the current cyber landscape and how international law applies to cyberspace. It is also unclear whether the group will be renewed at the end of its current mandate (2019–2020) or whether other mechanisms may be more suitable to facilitate institutional dialogue on cyber issues. The details of the GGE discussions are not yet public, but the group has until September 2021 to finalise its report for the UN General Assembly. Read more on page 7.

Ultimately, the two UN groups and similar initiatives will not succeed without a willingness on the part of the major actors in the digital field to seek win-win international solutions as a way to avoid cyber-conflicts and prevent further deterioration of the global digital space. While most actors will benefit from global cooperation on cybersecurity, future progress will require careful management of the interplay between power politics, the differing perceptions and priorities of various actors, and a range of potential strategic (mis)calculations. In the meantime continued international dialogue will be essential, for which the two UN groups provide a model.

To stay up-to-date with developments in the digital health field, follow the dedicated page on the Digital Watch observatory.
Digital policy developments in February

The digital policy landscape is filled with new initiatives, evolving regulatory frameworks, and new legislation and court judgments. In the Digital Watch observatory – available at dig.watch – we decode, contextualise, and analyse ongoing developments, offering a digestible yet authoritative update on the complex world of digital policy. The monthly barometer tracks and compares the issues to reveal new trends and to allow them to be understood relative to those of previous months. The following is a summarised version; read more about each development by clicking the blue icons, or by visiting the Updates section on the observatory.

Global IG architecture
The Multistakeholder Advisory Group decided that this year’s Internet Governance Forum (IGF) will address environmental issues in addition to those surrounding data, inclusion, and trust. The OEWG and the GGE held their second sessions.

Sustainable development
The United Nations Economic Commission for Africa urged African states to adjust their development strategies to the digital age. The Belgian Development Agency and telecom company SES signed an agreement to deliver satellite connectivity to 20 African countries. North Macedonia and Scotland are exploring digital ID solutions.

Security
A cyber-attack disrupted Internet connectivity in Iran. In the USA, a hack affecting MGM Resorts exposed the data of 10 million guests. Georgia, the UK, the USA, and the Netherlands accused Russia of being behind the 2019 cyber-attack that affected Georgia. Russia denied the accusations. It emerged that US and German intelligence have spied on other countries for decades through rigged encryption equipment. Brazil launched a cybersecurity strategy to protect the country from cyber-threats. Facebook announced new parental control tools for its Messenger app. UNICEF and Bangladesh launched a partnership to train one million children in online safety.

E-commerce & Internet economy
As part of ongoing antitrust investigations, the US Federal Trade Commission (FTC) ordered Amazon, Apple, Facebook, Google, and Microsoft to hand over detailed information on hundreds of acquisitions made over the past decade. The US government issued a new 45-day extension allowing Huawei to buy technology from US companies. G20 finance ministers reiterated their commitment to reaching a consensus-based solution on taxation in the digital economy by the end of 2020. The Spanish government approved a 3% digital services tax which is now to be discussed in parliament. Sweden started testing an e-krona, a move towards the creation of the world’s first central bank digital currency.
Digital rights
The Office of the Privacy Commissioner of Canada took Facebook to court over its privacy practices. The New Mexico attorney general sued Google for collecting student data through Chromebooks. The Irish Data Protection Commission launched inquiries into Google and Tinder.

Facebook, Google, and YouTube asked facial recognition company Clearview AI to stop scraping photos from their platforms. The company also faces a second class-action lawsuit in the USA and is under investigation by Canadian privacy commissioners.

The European Data Protection Board warned that Google’s acquisition of Fitbit has privacy implications.

New Internet shutdowns were reported in Myanmar’s Rakhine and Chin states.

Jurisdiction & legal issues
A Dutch court ruled that a government system using AI to identify potential welfare fraudsters is in violation of human rights laws. A Russian court fined Twitter and Facebook for breaching data localisation regulations.

The European Court of Human Rights ruled that indefinite data retention violates privacy.

Huawei and its subsidiaries were charged with racketeering and theft of trade secrets in the USA.

Ethiopia passed a law on online disinformation and hate speech. The German government approved an online hate speech bill.

Facebook proposed a series of principles to guide future regulations targeting online platforms.

Infrastructure
Google announced the shutdown of its free wi-fi Google Station programme.

Qualcomm announced the design of chips that can connect mobile phones to disparate 5G networks.

Sweden indicated it will not exclude Huawei from its 5G rollout plans. Huawei promised ‘5G for Europe made in Europe.’ The USA warned that alliances will be at risk if countries use Huawei 5G technology.

The controversy over the proposed sale of the .org registry continued.

New technologies (IoT, AI, etc.)

Signatories of the Rome Call for AI Ethics committed to promoting ‘algor-ethics.’

Twitter introduced a new policy for dealing with deepfakes on its platform.

The Dutch government launched a campaign to encourage people to update their smart devices. Australia published a national blockchain roadmap.

In the USA the White House proposed increased funds for AI and quantum research for fiscal year 2021. India launched a National Mission on Quantum Technologies and Applications with a budget of approximately US$1 billion over five years.
Coronavirus: Why and how is it a digital issue?

‘AI sent first coronavirus alert, but underestimated the danger’ Drug makers are using AI to help find an answer to the coronavirus WHO says fake coronavirus claims causing “infodemic” recent headlines make it clear that the coronavirus outbreak has serious implications across several areas of digital policy.

Data to the rescue

Real-time data collection and analysis is crucial in the early detection and monitoring of public health emergencies, as well as in ongoing risk assessment and developing concrete measures to address outbreaks.

It was real-time data processing that led to the identification of the coronavirus outbreak and its potential to develop into an epidemic or pandemic. Canadian AI company BlueDot collects and analyses an enormous amount of unstructured data pertaining to global health on an ongoing basis, including flight records and climate information, which enabled them to provide an early warning to the World Health Organization (WHO).

Yet room for improvement remains, and new initiatives on cross-border data sharing have emerged alongside calls for others. The Director-General of WHO, Tedros Adhanom Ghebreyesus, invited the health ministers of member states to collaborate on improving data sharing practices regarding the coronavirus and in general. Academia and the private sector are also involved: Significant data has been shared through Harvard Medical School’s Github, by the Institute of Health Metrics and Evaluation, and by risk analysis firm Metabiota, among others.

Data visualisation has also been put to use in tracking the spread of the disease. A notable example is the tool developed by the Center for Systems Science and Engineering at Johns Hopkins University to combat what the Washington Post called ‘a pandemic of misinformation about coronavirus’ or ‘infodemic’.

Putting our faith in AI

Major tech companies and medical and scientific institutions alike have turned to AI in efforts to halt the spread of the disease. BlueDot’s AI-powered algorithms predicted the outbreak days before WHO issued an alert, and AI is also being employed in other prevention measures. Chinese AI companies Magvii and Baidu have installed AI-powered scanners across several subway stations in Beijing to detect passengers’ body temperatures. Similarly, Integrated Health Information systems (IHiS) in Singapore is reported to be piloting iThermo, an AI-powered temperature screening tool able to identify individuals with symptoms of fever.

However, AI has serious limitations as well. Faulty data and external factors not taken into consideration by AI algorithms can contribute to the spread of the so-called ‘infodemic’. For instance, one AI-powered simulation predicted that the coronavirus could infect 2.5 billion people and kill as many as 52.9 million, on the basis of data released by China; this prediction vastly overestimates the scale of the outbreak so far.

Fake news on the rise

Measures to regulate coronavirus-related digital content and contain the ‘infodemic’ have been initiated by both WHO and major tech companies such as Facebook and Google. WHO has a dedicated ‘myth busters’ page to address popular myths related to the spread of the disease, and Google’s efforts to address the issue include the activation of an ‘SOS alert’ in results for searches linked to coronavirus. Facebook is attempting to curb the spread of misinformation by removing false assertions and virus-related conspiracy theories posted on its social media platforms.

Cybercriminals exploit fear

Coronavirus is also causing concern in the realm of cybersecurity. Cybercriminals are reported to be seeking to exploit public anxiety to distribute malware. For instance, Sophos Security has identified a phishing scam impersonating WHO that uses sensationalist false information about coronavirus as bait.

For a more detailed analysis of the digital policy aspects of the COVID-19 outbreak, follow the dedicated page on the GIP Digital Watch observatory.
OEWG continues discussions on cyber norms

The UN Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security held its second substantive session on 10–14 February in New York. Here we look at how the group’s discussions on responsible state behaviour in cyberspace unfolded, identifying areas of convergence and divergence as well as next steps.

Areas of convergence

Delegations discussed which regional confidence-building measures (CBMs) are ready to be recognised at the global level, and for the most part praised the capacity building work undertaken by the Organization for Security and Co-operation in Europe, the Association of Southeast Asian Nations, and the Organization of American States. Suggestions for a global repository of CBMs, as well as a global repository of points of contact for cyber-incidents, were well received. Some questions remain, however, such as who would manage such repositories, with Ghana suggesting that it could be a task for the OEWG itself.

There was general agreement that capacity building should be demand-driven, needs- and evidence-based, and non-discriminatory, and that it should bridge digital and gender divides. The potential for synergies between capacity building, CBMs and norms was underlined, and its potential role in achieving sustainable development goals (SDGs) was stressed by Norway, Estonia, Nicaragua, and the Netherlands. The UN, the Global Forum on Cyber Expertise, and the IGF were suggested as potential fora for continuing discussions on capacity building.

Regarding future institutional dialogue, several states expressed support for the creation of a new mechanism or platform, under the auspices of the UN, that would allow participation on the part of all stakeholders in discussions on cyber issues, but the majority expressed scepticism regarding the creation of any such additional institutional mechanism. Several delegations noted that they consider OEWG and GGE processes themselves as forms of institutional dialogue, and Russia proposed that the OEWG’s mandate should be renewed beyond 2020.

Areas of divergence

Delegates were polarised over the question of whether new norms are needed. The majority agreed that the norms described in the 2015 GGE report should be implemented. However, a number of delegates proposed additional measures for the OEWG to consider: (a) norms that would elaborate on the existing GGE norm regarding the protection of critical infrastructure; (b) a new norm on refraining from weaponisation and offensive uses of ICTs; (c) norms laid out in the Shanghai Cooperation Organization proposals of 2011 and 2015; and (d) new measures to address threats emanating from online content.

Positions also diverged on the applicability of international law to cyberspace. Most delegates agreed that the OEWG should clarify how existing international law applies to cyberspace, and Mexico suggested that the International Law Commission should conduct a study on the issue. Syria and Russia questioned the applicability of international law online, however, with the latter also expressing doubts regarding the application of humanitarian law in peacetime and in hybrid warfare. Calls for a new treaty specific to cyberspace came from Iran, Egypt, Syria, and Indonesia. The applicability in cyberspace of Article 51 of the UN Charter, enshrining the right to national self-defence, was also discussed. Brazil and India noted that it is unclear what threshold cyber-attacks would need to reach for the article to be invoked. Russia took a firmer stance and asserted that the article applies only in the context of an armed attack, and that a cyber-attack is not an armed attack.

Next steps

The OEWG Chair noted that the pre-draft of the group’s report would be circulated to delegations at the beginning of March. On 30–31 March, delegates will have the opportunity to comment on the pre-draft report during the first informal intersessional exchange. The second informal intersessional exchange on 28–29 May will give delegates the chance to comment on the revised pre-draft report. Negotiations over the draft report will take place during the OEWG’s third substantive session on 6–10 July.

The OEWG will report to the 75th session of the UN General Assembly in September 2020. The Chair stated that since the OEWG is an intergovernmental process governments will ultimately decide on the content of the report, but contributions from other stakeholders are welcome.

For a more in-depth summary of the OEWG discussions, read our session reports.
Human-centric AI: building trust through regulations

It is often noted that the EU’s focus on upholding human values and fundamental rights is one of its key digital assets. It is therefore not surprising that trustworthiness and a human-centric approach are core elements in the European Commission’s plans to accelerate the development and use of AI in Europe.

Fostering and maintaining trust in technology is never an easy task. This is especially the case with AI applications that have potential implications for core European values and fundamental rights such as human dignity and privacy. It is the Commission’s view that trust in AI can be built through a clear European regulatory framework, but what would that mean in practice?

Existing EU rules and regulations in several areas (product safety, liability, consumer rights, fundamental rights, etc.) are already relevant to AI applications and could be improved to cover certain AI-specific risks and situations. But they may not be sufficient to address the full range of challenges associated with AI, so the Commission proposes that new legislation be developed for high-risk AI applications. An application would be defined as high-risk if it operated in a high-risk sector and if its intended uses were deemed to pose significant dangers (for example) to public safety or consumer or fundamental rights. Standards of robustness and accuracy would be imposed, with human oversight another possible measure.

Regulation may be necessary to ensure trustworthiness in AI, but it should not stifle innovation. The Commission seems to be aware of this risk, noting that any new legislation should not be excessively prescriptive nor create disproportionate compliance burdens (especially for SMEs). As with other areas of regulation, one key challenge will be achieving a balance between the rights of users and the interests of the private sector.

Leadership in the data economy: creating European data spaces

One of the European Commission’s priorities is to secure for the EU a leading role in the data economy. Though many of the prerequisites are in place (the EU ‘has the technology, the know-how and a highly skilled workforce’), improvements are needed in one area in particular: access to data.

To that end the Commission proposes the creation of a single European data space that would facilitate access to and the re-use of public and private data from the EU and beyond, as well as sector-specific versions. For example, common European data spaces in manufacturing, health, and energy would enhance the competitiveness and sustainability of these sectors.

The prospect of a single European data space promises to ensure easy and secure access to high-quality data...
from public and private sectors alike, and thus to foster innovation and economic growth. But how willing will the private sector be to share (more) data, and how easy will it be to convince public authorities to do the same? These are important questions given companies’ current reluctance to share data with one another (on grounds of competitiveness, for instance) and the challenges involved in making government-held data public. In the Commission’s view, the answer could be a new data governance framework to facilitate cross-border data sharing, introduce interoperability requirements and standards, and specify the different scenarios in which various kinds of data could be used.

Public trust is essential here as well. As the common data spaces will also contain personal data, one key challenge is to balance the free flow and use of data with information security and individual privacy. This challenge will be complicated further if, as the Commission envisions, a new data paradigm is emerging in which more data is stored and processed closer to the user (‘at the edge’). The Commission’s proposed solution is to give users more control of their data and to empower them to decide at a granular level what is done with it.

Towards European excellence: strengthening the foundations

The EU wants to achieve technological sovereignty and to be a global leader in AI and the data economy. To these ends new legislation and governance frameworks are being explored, but the Commission acknowledges that more needs to be done as well to strengthen the foundations on which tech sovereignty and a global leadership position are to be built: infrastructure, research and development (R&D), education, and market competition.

A strong and sustainable data economy can only be developed if secure, resilient, and advanced digital infrastructures are in place. For that reason, the Commission is planning to allocate more funds to and encourage increased public and private investment in areas such as gigabit connectivity, secure fibre and 5G infrastructures, supercomputing, quantum computing, and blockchain. It also recognises that R&D activities will be essential in keeping the EU at the forefront of digital progress. In the field of AI, for example, the Commission proposes excellence and testing centres to ‘retain and attract the best researchers and develop the best technology’.

Investing in skills to ensure that the workforce is prepared to support the EU’s ambitions is another priority. A Digital Education Plan and a more robust Skills Agenda will be developed to increase digital competence across Europe and to ensure that the demand for workers highly skilled in digital technologies can be fully met.

It is also essential that the European digital market is both open and fair. Here the focus should be on ensuring that competition, antitrust, and taxation rules are fit for purpose in the fast-changing digital world and create a level playing field for EU and non-EU players alike.

These efforts will lay the foundation for the Commission’s endeavours to ensure that Europe excels and provides leadership in the data economy. If implemented carefully, they may indeed lead to the intended outcomes. But negative unintended consequences may also arise: market and regulatory fragmentation, for instance, or regulatory burdens that stifle innovation. To avoid them the Commission must give careful consideration to input and feedback from individuals, companies, public institutions, and other stakeholders that participate in the public consultations.
Policy discussions in Geneva

Each month Geneva hosts a diverse range of policy discussions in various forums. The following updates cover the main events in February. For event reports, visit the Past Events section on the GIP Digital Watch observatory.

Collecting data: How can big data contribute to leaving no one behind and achieving the SDGs? | 19 February 2020

The Road to Bern via Geneva initiative, began with a first dialogue focused on data collection issues, co-organised by the World Meteorological Organization and WHO. This and subsequent dialogues – on data security (13 March), data commons (30 April), and the use of data (23 June) – will feed into the 2020 UN World Data Summit (18–21 October, Bern).

During this first dialogue, more than 100 diplomats and experts emphasised the lack of common principles, norms, and standards in the collection and processing of data in International Geneva and beyond. A key challenge in the use of data in achieving the SDGs was raised, namely the difficulty of collecting data regarding vulnerable populations in remote areas.

The initiative is organised by the Permanent Mission of Switzerland to the UN in Geneva and the Geneva Internet Platform (GIP), with the participation of international organisations, permanent missions, the tech community, civil society organisations, and the press.

Read our session report for a summary of the discussions.

Collecting data: How can big data contribute to leaving no one behind and achieving the SDGs? | 19 February 2020

Join us for the next dialogue on 13 March 2020, on the theme ‘Protecting data against vulnerabilities: questions of trust, security, and privacy of data’

Participants will explore practices, needs, and challenges related to protecting data, while also trying to identify new actors and new approaches that could ensure better data security and individual privacy.

Human rights in the context of cybersecurity | 26 February 2020

Organised by Ghana, the Netherlands, and Estonia, the event explored issues relating to the application and violation of human rights in cyberspace. The discussion was held on the margins of the 43rd session of the Human Rights Council and the second session of the UN GGE.

Speakers emphasised the need for greater awareness of human rights and their violation in cyberspace, especially with Internet shutdowns and restrictions as well as online surveillance hindering the exercise of fundamental freedoms. Not only do such measures and practices erode traditional human rights (the right to privacy, freedom of expression and assembly online, etc.) but also others, such as freedom of movement and self-sovereignty, may be less familiar to many.

Considering the roles and responsibilities of various actors in cyberspace, participants underscored that governments, the private sector, and civil society all need to promote and uphold human rights in the digital environment.

They also stressed that the role of tech companies needs to be defined with more clarity, given that digital security is to a considerable degree in the hands of corporations. Diverging views on the applicability of international law in cyberspace were also discussed.

Finally, repeated emphasis was given to the importance of identifying new avenues for dialogue and cooperation between the cybersecurity and human rights communities.

Read our session report.
The main global digital policy events in March

Here we take a look ahead at the digital policy calendar to highlight the main discussions taking place in the next few weeks across the globe. For more detail and for the proceedings of some events – including reports from individual sessions and a final report summarising the discussions – please check in regularly to the Digital Watch observatory.

7–12 MARCH
ICANN 67 (online)

The community forum will give ICANN’s supporting organisations, advisory committees, and the broader community the opportunity to discuss various issues pertaining to ICANN’s activity and the management of the domain name system (DNS). New generic top-level domains, DNS security and stability, and privacy in the context of domain name registration are among the topics expected to be discussed. The meeting will be held exclusively online, due to the coronavirus outbreak.

16–17 MARCH
AI Summit 2020 (Brussels, Belgium)

Organised by POLITICO for the third consecutive year, the summit will host a range of discussions on the future of AI technology and its global regulation. The emphasis will be on the question of whether and how the EU can become a global player on the international AI scene, with regard to both the development and regulation of AI technologies.

23–27 MARCH
23rd Session of the Commission on Science and Technology for Development (Geneva, Switzerland)

At its 23rd session the Commission will focus on two key questions: (1) how to harness rapid technological change for inclusive and sustainable development; and (2) space technologies’ potential to contribute to sustainable development, as well as the need for international research collaboration in this context. In addition, the Commission will review progress in the implementation of the outcomes of the World Summit on the Information Society.

9–10 MARCH
Crypto Assets Conference 2020 (Frankfurt, Germany)

The conference will bring together technology experts, industry innovators, crypto investors, and blockchain entrepreneurs to discuss developments related to blockchain and crypto-assets. Key topics will include custody of digital assets, bitcoin and other crypto assets, tokenised securities and securitised tokens, the prospect of a digital Euro, machine-to-machine payment processes, and blockchain-related regulatory developments.

17–18 MARCH
Blockchain Expo Global 2020 (London, UK)

Both exhibition and conference, the event will showcase cutting-edge technologies (in blockchain, IoT, 5G, cybersecurity and cloud, AI and big data) and provide a forum for discussions of these technologies’ applications and implications. Topics to be addressed include IoT as a driver of digital transformation, the evolution of national cyber-threats, token economies, the challenges of autonomous systems, and AI for good.

25 MARCH
European AI Policy Conference (Brussels, Belgium)

Hosted by the Center for Data Innovation, this conference will bring together a range of European stakeholders to explore advances in AI and discuss prospective policies to support the development and uptake of AI in Europe. Some of the topics to be addressed include: why European success in AI is essential, how the EU compares to other world leaders in the field, and what steps European policymakers should take to make the EU more competitive.
Behind Diplo’s AI Lab

Diplo’s AI Lab conducts machine learning (ML) experiments to gain insights into AI before analysing possible AI governance solutions. It also develops new tools for diplomatic reporting, complex analysis, and policy foresight.

ML is a high-tech but essentially straightforward process: for instance, over several iterations of feedback and corrective adjustment, an AI-system can ‘learn’ to simulate human writing. The image below illustrates the stages involved.

---

**Promotion**

**About this issue**

Issue no. 47 of the *Digital Watch* newsletter, published on 3 March 2020 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđelković, Andrijana Gavrilović, Jovan Kurbalija, Marco Lotti, Nataša Perućica, Vladimir Radunović, Sorina Teleanu | Editing: Abe Davies | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo’s CreativeLab | Get in touch: digitalwatch@diplomacy.edu

**Go deeper**

Click the blue icon wherever it appears in the digital version to access a source and/or further resources.

**On the cover**

Coronavirus: The role of digital tech & policy. Credit: Vladimir Veljasević

© DiploFoundation (2020) https://creativecommons.org/licenses/by-nc-nd/4.0/

---

The Geneva Internet Platform is an initiative of: