Geneva Internet Platform



You receive hundreds of pieces of information on digital policy. We receive them, too. We decode, contextualise, and analyse them. Then we summarise them for you.

OUR PREDICTIONS: DIGITAL POLICY IN 2019

The digital realm is mirroring societal developments. Cyber risks and uncertainties are growing. A cyber-arms race is in the making. Opportunity-wise, artificial intelligence (AI), quantum computing, and blockchain are spearheading a wave of new applications in health, agriculture, and development. In 2019, the digital realpolitik trend will accelerate, and there are 10 areas of development which we will need to watch closely.

1. Data governance: Discussions will mature amid tensions

As data continues to oil the modern economy, the contentious issues surrounding cross-border data rules will intensify. Policymakers will continue their quest for data governance solutions that balance the interests of the private sector, users, and law enforcement agencies (LEAs). Moreover, the variety of data (personal, business, scientific, etc.) will be increasingly reflected in varied data regulation worldwide. For example, security data is likely to be kept under national jurisdictions, while business and scientific data will flow more easily across national borders. Likewise, the trend of diversification of data policies of the major tech companies will continue.

2. Digital geo-economics: The race for tech dominance will continue

The China–US trade war is set to continue this year. Behind the tensions are both countries' ambitious plans in tech sector: President Trump's pledge to 'make America great again' runs parallel to President Xi's 'Made in China 2025 plan'. These plans could lead to more state influence over firms and impact competition in the digital economy worldwide. As the two presidents have agreed to halt new trade tariffs for 90 days to allow for talks, all eyes will be on these talks between the two countries.

3. Geo-politics: A security and cyber-arms race in the making

The cyber-arms race will accelerate in 2019, as countries continue to develop offensive cyber capabilities. One main question is likely to be discussed in both multilateral and



IN THIS ISSUE GENEVA Artificial intelligence and diplomacy, the future of work, digital co-operation, and stability in cyberspace were among the topics tackled in January discussions. More on page 2 OBSERVATORY Security, the Internet economy, digital rights, and jurisdiction were prominent this month. Read the latest updates. More on pages 4–5 (📋 **CYBERSECURIT** Two UN groups will further explore issues related to responsible state behaviour in cyberspace. What can we expect? More on page 6 (📋 **CRYPTOCURRENCIES** How are countries around the world regulating cryptocurrencies and crypto-assets? Read our summary of the main trends. More on page 7 📋

Issue no. 37 of the *Digital Watch* newsletter, published on 6 February 2019, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors:
Stephanie Borg Psaila (Editor), Efrat Daskal, Andre Edwards, Arvin Kamberi, Marco Lotti, Nataša Perućica, Ilona Stadnik, Sorina Teleanu | Design
by Viktor Mijatović, layout by Aleksandar Nedeljkov, Diplo's CreativeLab | In addition to the *Digital Watch* newsletter, read our in-depth coverage of
developments on the *GIP Digital Watch* observatory (https://dig.watch) and join our online briefing on the last Tuesday of every month (https://
dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu | Download your copy at https://dig.watch/newsletter/january2019

Predictions continue on page 3 📋

GENEVA



DIGITAL DEVELOPMENTS IN GENEVA

Many policy discussions take place in Geneva every month. The following updates cover the main events of the month. For event reports, visit the Past Events section on the *GIP Digital Watch* observatory.

Science fiction meets policy | Policy meets science fiction Identified as a tentative process of cross-fertilisation, this event that took place on 15 January addressed the question: What can sci-fi teach us about digital politics and its future? With the interdisciplinary participation of policymakers, diplomats, designers, writers, it brought different ways of thinking to the international architecture of Geneva in an attempt to identify major digital trends in the near future. The final part of the workshop consisted of four parallel interactive sessions. The groups were led by experts who zoomed in on sci-fi and digital politics from different perspectives and provided hands-on practical exercises to challenge participants to think outside the box. *Read the event report*.

AI and the Law Public Conference The AI and the Law public conference, which took place on 16 January, was organised by the Law Faculty of the University of Geneva in collaboration with the Geneva-Harvard-Renmin-Sydney Platform. The conference tackled issues raised by the evolution and development of AI, focusing specifically on the latest developments in robotics. So-called smart robots are now able to interact with humans and the environment, in addition to being able to learn, adapt, evolve, and therefore make autonomous decisions. The conference featured discussions on the global impact of AI on the law, the concept of choice and optimisation, the identification of state responsibility in case of cyber-attacks, and finally, on the humanitarian implications of the use of AI.

Launch of the International Labour Organization Global Commission on the Future of Work report On 22 January, on the occasion of its centenary, the ILO Commission on the Future of Work published its report *Work for a brighter future*.¹² The Commission was composed of 27 members from leading figures of the business and labour sector, think tanks, academia, and non-governmental organisations. In the report, the Commission calls for a human-centred agenda for a decent future of work, issuing ten key recommendations and pushing for the provision of a universal labour guarantee, a social protection guarantee, and a lifelong learning guarantee, among others. Challenges caused by new technology and climate change are taken into account and the need to find a collective response to these issues is emphasised in order to avoid potential negative impacts on the future of work. Experts recognised the risk of job losses caused by AI and automation but also pointed out the potential of these technologies for the creation of new jobs if implemented investing in people's capabilities and the existing institutions of work.

De-Briefing of the meetings of the UN High-Level Panel on Digital Cooperation and the Global Commission on Stability in Cyberspace On 25 January, the GIP hosted a debriefing on the meetings of the United Nations Secretary General's High-Level Panel on Digital Cooperation (HLP.DC) and the Global Commission on Stability in Cyberspace (GCSC). After four months of intensive public consultations and discussions, the HLP.DC started drafting its report and recommendations during the Geneva meeting (21-22 January). The Panel will hold another round of consultations on the draft report and recommendations. The final report will be submitted to the UN Secretary General on 31st May. The GCSC is a multistakeholder initiative formed by a selected group of experts working to make sure that silos can make a more informed decision and avoid norm collision. The work of the Commission follows a bottom-up approach which starts by considering the politically binding norms in cyberspace (e.g. the core beliefs shared within a multistakeholder environment). At present, the GCSC has a working definition of cyber stability that is still under revision. The Commission is currently open to suggestions about cyber stability, and it is expected to make final recommendations by the end of 2019. *Read the event report*.

The launch of the World Intellectual Property Organization report on Al On 31 January, WIPO launched its first 'Technology Trends' report, on AL^{IZ} which shows that there has been a significant increase in AI-based inventions and patent filing, and that the technology is making its way into mainstream markets. It further identifies the most active stakeholders in AI technology development from industry and academia as well as the geographical distribution of AI patent protection. AI patents are mostly filed by US companies; IBM and Microsoft are named as having the largest AI portfolio in terms of patent applications. Most patent filings concern machine learning techniques.

ANALYSIS

DigitalWatch

OUR PREDICTIONS: DIGITAL POLICY IN 2019

Continued from page 1

multistakeholder processes: Where do we draw the line with armament and the use of cyber-capabilities? Cyber intrusions and subversions under the threshold of armed attack will probably increase, and so will the open attributions and accusations. The lack of clear evidence for attribution may, however, bring about co-operation in establishing certain common methodologies for attribution.

4. Artificial intelligence: Maturing beyond hype

The discussion around AI is expected to mature and move beyond the hype, including within policy spheres. We can expect more countries to create national AI strategies, while international entities will continue the debate on issues such as ethics and human rights, the future of work, and lethal autonomous weapons (LAWs). Safety and security issues around autonomous cars will become more prominent. Questions around liability and a possible legal status for autonomous systems are also likely to remain in focus in 2019.

5. Security will be omnipresent

With their increased reliance on IT infrastructures and data, it is expected that companies will take cybersecurity even more seriously, feeding a fast-growing market for cyberinsurance. The security of the Internet of Things (IoT) will need to be given closer attention, as smart devices become more commonly used. We can also expect stronger calls for national regulation on higher security standards, as well as more pressure from governments for lawful access to data to help with cybercrime investigations. The question of anonymity on the Internet will also likely resurface.

6. Tech companies: The dawn of government regulation

The market power and influence of giant Internet companies have made policymakers very uncomfortable. 2018 ushered in a new wave of regulation on issues such as taxation, Internet intermediaries' responsibility, and data localisation requirements. As demonstrated at this year's World Economic Forum (WEF), the call for government regulation is expected to continue. The main question is whether countries will agree on global rules, or will go at it alone. As the trend from 2018 showed, more and more countries are taking action unilaterally, bilaterally, and regionally.

7. Global e-commerce rules will hang in the balance

After years of failed attempts to start negotiations within the World Trade Organization (WTO) on a set of e-commerce rules, over 70 countries agreed to start the talks in March. It will not be smooth sailing though, as strong divergences already exist.²² From a regulatory perspective, the relevance of global rules will depend on how fast countries will manage to pen a WTO agreement. And while member states grapple with negotiations, regional deals will continue to exert control over trade and investment, demonstrating, once again, that geography matters.

8. Hardware is back

For some time, most digital policy discussions focused on software and data. But in 2019, we can expect more focus on hardware. The increasing relevance of microchips in the modern economy² will drive countries to push for selfreliance on domestic production. There will be more discussions on standardisation and security issues around IoT sensors and devices. The deployment of 5G networks will accelerate in 2019, supporting new applications, but also generating new debates on spectrum policies. Quantum computing will gain momentum, as countries and companies continue research in this area.

9. Blockchain and cryptocurrencies: A year of reckoning

After a lot of hype around the potential of blockchain, 2019 will be a year of reckoning. Experiments will be reviewed and assessed, and those with an interest in the technology will need to decide whether to sustain it. Cryptocurrencies are also in hot water after the losses suffered by some of them. While experts say that their volatility is a natural characteristic, policymakers remain less optimistic. The overall regulatory trend is to properly recognise different types of cryptocurrencies and to update financial rules to classify new digital financial assets. *More on page* 7.

10. Digital identities will catch on

Questions of identity of individuals, groups, and nations are behind many political controversies worldwide. Identity issues are spilling over from real to digital issues with many possibilities, some risks, and a few dilemmas. In 2019, many countries will search for solutions to develop digital identity systems, and India's Aadhaar and the India Stacks approach are expected to serve as an inspiration for many. On the private sector side, the power that Internet companies gain from becoming providers of digital identities will continue to attract the attention of policymakers.

These predictions are based on DiploFoundation's 'crystal ball' exercise. Read the full text of the predictions for digital policy in 2019.

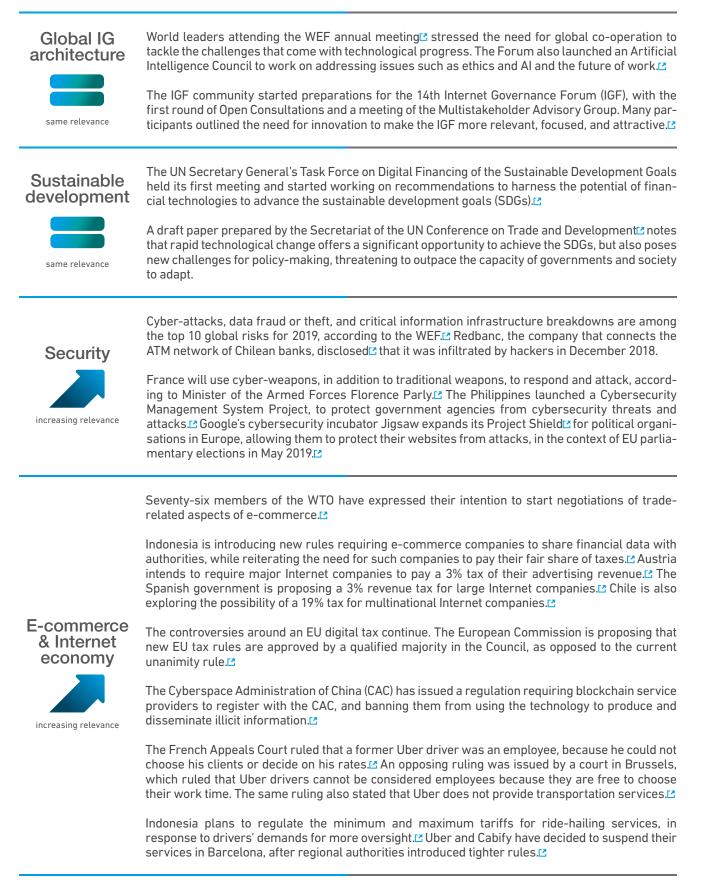


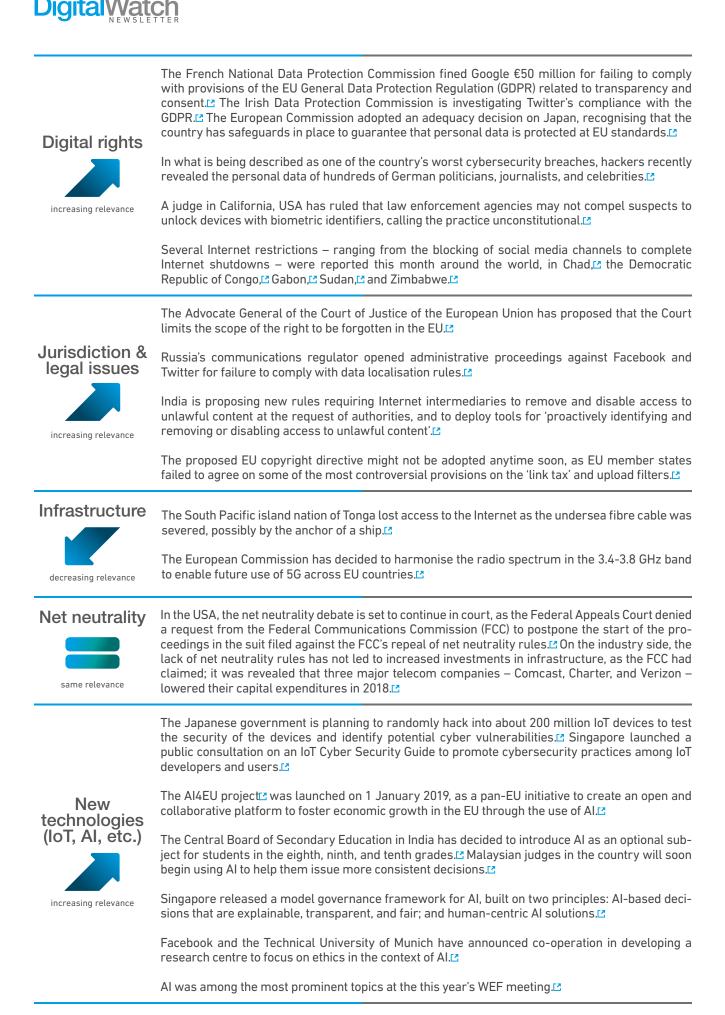


OBSERVATORY

DIGITAL POLICY: DEVELOPMENTS IN JANUARY

The monthly Internet Governance Barometer tracks specific Internet governance (IG) issues in the public policy debate, and reveals focal trends by comparing issues every month. The barometer determines the presence of specific IG issues in comparison to the previous month. *Read more about each update*.





ANALYSIS

DigitalWatch

DISCUSSING STATE BEHAVIOUR IN CYBERSPACE: WHAT SHOULD WE EXPECT?

In December 2018, the UN General Assembly approved the creation of two distinct groups to further explore issues related to responsible state behaviour in cyberspace: an Open-Ended Working group (OEWG) and a new Group of Governmental Experts (GGE). The two groups were proposed in resolutions put forward by Russia and the USA, respectively. What are their mandates, and what can we expect from these groups?

How the mandates compare

Proposed by Russia, the OEWG will start its work in June 2019. Its composition is declared as open, implying that it will include all UN member states that express a desire to participate. The main task of the group will be to further develop norms, rules, and principles of responsible state behaviour, and ways to implement them, as well as to study the possibility of institutionalising the dialogue on the application of international law on a regular basis under the auspices of the UN. Also included in the group's mandate is a study of existing and potential threats to information security and possible confidence-building measures and capacity-building. The OEWG will work on a consensual basis to develop its report, which is to be presented at the 75th UN session, in autumn 2020.

The GGE, proposed by the USA, I is designed for a longer period – three years – and will continue the activities of the previous GGE, is studying further possible joint measures to address threats in the field of international information security, including norms and rules of responsible behavior, as well as the application of international law to the use of ICT by states. The result will be a report that does not imply the consensus of all participants, but must contain an annex in which the GGE members will include their national positions on the application of international law in the ICT environment.

One notable difference between the two groups is related to their composition. The OEWG is to involve all interested UN member states and also hold 'intersessional consultative meetings' with businesses, non-governmental organisations, and academia. The GGE is taking a more intergovernmental path: It will have limited participation from member states, on the basis of 'equitable geographic distribution', and will hold consultations with regional inter-governmental organisations and all UN member states.

Prospects for both groups

The creation of two separate groups to discuss international information security issues has attracted different reactions. Some member states are concerned that the two parallel tracks could lead to less effectiveness, while others have noted that the processes are in fact compatible.¹⁷ In reality, both groups have advantages and disadvantages.

The OEWG format has many advantages. The resolution it is based on already includes a list of particular norms to be further developed, so it is possible for the group to focus its discussion on ways and mechanisms of their implementation. The open composition of the group allows every member state to participate, in contrast to the limited number of members of the previous GGEs. The rule of consensus decision-making will ensure that the common interests of all participants will be included in the final document. Also, the time factor plays a crucial role – the report will be submitted in two years, faster than the report of the GGE.

But there are also several disadvantages. The open composition does not imply the participation of key countries 'by default', thus the composition of the group may be much smaller than desired. For example, countries that did not vote for this resolution may be less likely to participate. The mandatory consensus can play a blocking role, or significantly affect the final wording of the report, making it more general in scope, unless the group consists of like-minded states who agree on issues of international information security. Finally, the involvement of other stakeholders in the exchange of views on the issue strikes a 'good tone' today. But significant challenges could appear in attracting the involvement of relevant actors from business and civil society.

The GGE format could be seen as having a strength in its principle of equitable geographical distribution in the selection of its members. A smaller group can be more efficient in its work as compared to a larger group. The absence of a binding consensus can also be viewed positively – the report would be submitted to the Secretary-General in any case. Regardless of what the group agrees on, the report will also contain national positions on the application of international law to the use of ICT by states. However, the group will need three years to submit a report, which can be seen as a significant drawback in an environment characterised by the continuous development of technologies and the emergence of new threats from ICT to international security.

Despite the creation of these two groups, states are still at the beginning of the development of legally binding norms of responsible behaviour in cyberspace. Of course, further progress will depend largely on the content of the report produced by the groups, but these documents will serve only as recommendations for states. Even if the work of both groups is successful, the probability of maintaining the polarisation of positions on international information security is still high, and the final goal may not be achieved.



6



IN FOCUS

CRYPTOCURRENCY AND CRYPTO-ASSETS: MAPPING THE REGULATION

In the past few months, we looked at the regulations around the world which are tackling cryptocurrencies and crypto-assets. With the help of publicly available data and other research sources, we mapped the regulations of around 140 countries and looked at the solutions implemented.

In our research, we looked separately at national regulations around cryptocurrencies, Initial Coin Offerings (ICOs), and/or online exchanges. What follows is a summary of our main findings.

Clarifying the terms

As with many novel technologies, first efforts are on track towards establishing a common taxonomy and topology for the cryptocurrency system. Apart from cryptocurrencies, crypto-assets are being recognised in many countries as a new financial instrument. This includes crypto tokens issued through the ICO processes. Many companies are using this method to raise money and the main issue for regulators is how to look at these tokens from an investment point of view. Central financial institutions are issuing recommendations for token classification and this is helping informed decisions around consumer protection concerns.

Tackling risks

Only a few countries have imposed a full ban on cryptocurrencies or ICOs. Policymakers are most oriented towards establishing clear procedures around online exchanges for cryptocurrency trading. Across the globe, regulators are enhancing the rules on Anti-Money-Laundering laws to append online cryptocurrency trading platforms. Almost all online exchanges are now implementing Know-Your-Customer procedures. The anonymity of cryptocurrency traders is almost non-existent.

Addressing financial concerns

Central banks around the world are being particularly careful about the public risks associated with the use of

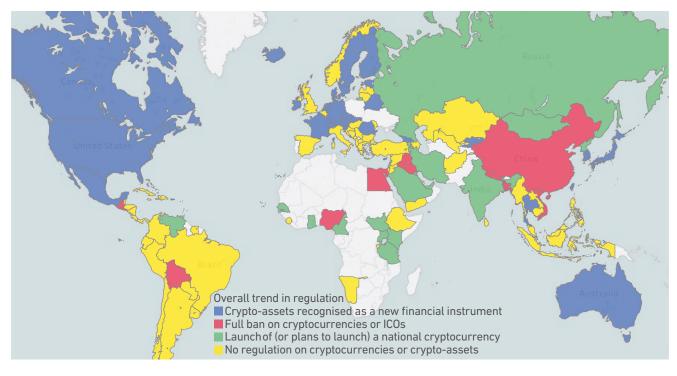
cryptocurrencies, and almost all have issued warnings on the risks involved in cryptocurrency trading. Tax rules are are also being amended in many countries to include profits for trading cryptocurrencies.

Some of the countries under the toughest financial sanctions have introduced plans to create national cryptocurrencies as a way of circumventing those sanctions. Venezuela has created the state-backed cryptocurrency named Petro; other countries are considering this course. On the other hand, small states and states with more liberal financial rules are trying to leapfrog with progressive regulation and innovative solutions for blockchain-based services.

Identifying regional trends

The EU is focusing on tougher customer protection rules and more transparent user policies. Asia is looking at the model of self-regulation by the industry, while Africa is searching for better consumer protection regulations and a possible leverage of crypto industry towards wider financial inclusion. Latin America is divided between those who believe that cryptocurrencies will bring financial freedom (Venezuela) and those that are completely banning cryptocurrencies and their use (Bolivia). The MENA region (Middle East and North Africa) is being tough on cryptocurrencies, but quite open towards decentralised data ledger technologies, often called blockchains.

For a more in-depth analysis of each country, including sources to regulations and other information, visit our interactive map on the *GIP Digital Watch* observatory.

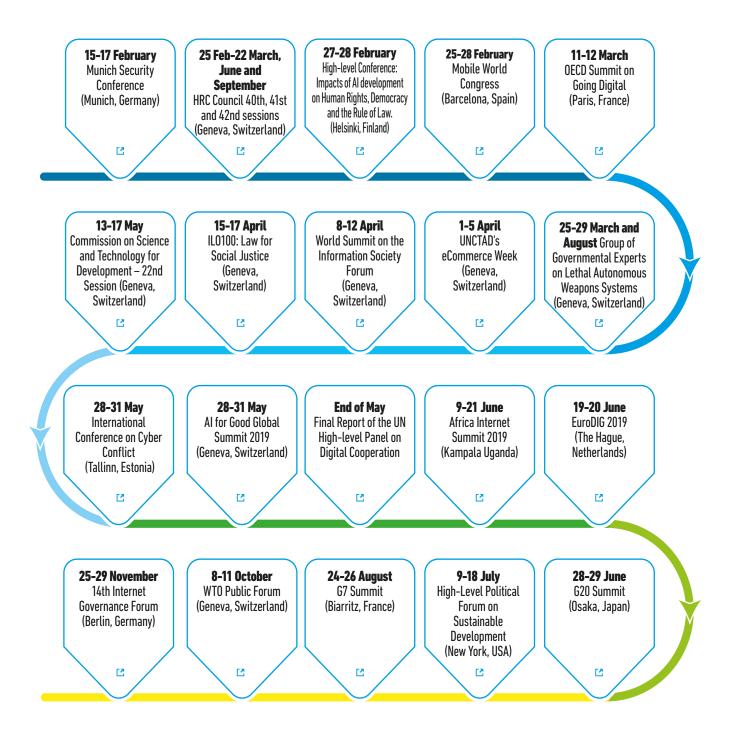




UPCOMING

THE MAIN DIGITAL POLICY EVENTS IN 2019

The events below – an extract from a very busy calendar of events – are likely to mark digital policy in 2019. While the list highlights events, in most cases they form part of processes which will run throughout the year. A full database of upcoming events and processes is available on the *GIP Digital Watch* observatory.



Scan the code to download the digital version of the newsletter.

