

## Celebrating 50 issues of timely updates on digital policy

020

50

06 2020

51

letter



# 50<sup>th</sup> issue



0

50

51

### TRENDS IN MAY

May's notable trends included regulations targeting social media platforms, ongoing privacy concerns around data tracing apps, and a renewed focus on cyber-attacks.

[Pages 2-3](#)

### TECH GEOPOLITICS

The role of technology in the geopolitical relations between the USA and China was emphasised in new US trade sanctions.

[Page 6](#)

### .ORG CONTROVERSY

ICANN rejected the proposed sale of the .org registry by the Internet Society to Ethos Capital. We look at some of the reactions and implications.

[Page 7](#)

### FUTURE OF MEETINGS

Hybrid meetings, which combine online and face-to-face interactions, will become the norm. How to adapt?

[Page 12](#)

# The top digital policy trends in May

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

## 1. New regulations target social media companies

Social media platforms have long been scrutinised over their potential responsibility for hosted content. The month of May brought several developments in this area.

The French Parliament adopted a law [requiring](#) online platforms to remove flagged hateful content within 24 hours, and child abuse and terrorist propaganda within 1 hour. If the online platforms fail to do so, they face fines of up to 4% of their global revenue. This law requires them to prevent the re-upload of removed content, and to establish complaint and appeal mechanisms for notifications of potentially illegal content. This law has been criticised by civil rights groups such as Article 19 [and](#) AccessNow [over](#) concerns that it may threaten freedom of online speech. They also criticise giving tech companies the power to determine what constitutes hate speech, as well as the fact that they need to monitor content to prevent re-uploads.

At the same time, four French anti-discrimination organisations have taken Twitter to court arguing that the company has not taken sufficient measures to remove hate speech from its platform. Claiming that the amount of hate speech on Twitter rose by 43% during the COVID-19 lockdown, the organisations have asked the court to designate an expert to audit Twitter's efforts to address this spike [.](#)

Twitter's action has triggered a policy controversy in the USA around the liability of tech platforms for the content they host. When President Trump posted tweets claiming that mail-in ballots are fraudulent, Twitter added a fact-check label to the posts and a link to a page describing the claims as 'unsubstantiated' [.](#) The company explained that the posts contained potentially misleading information about voting processes and had been labelled to provide additional context [.](#) In reaction, Trump accused Twitter of interfering in the US President elections and stifling free speech.

Amid these controversies, on 28 May, the US President issued an executive order [asking](#) for a review of the legislation which protects online platforms from being

### A double celebration

It's a double celebration for us at *Digital Watch*. We're marking the 50th edition of our newsletter, and five years since the *Digital Watch* observatory was set up. Time flies!

Our celebrations will run throughout June with blog posts, videos, and other content, culminating with the launch of the newly redesigned observatory on 30 June. Join us for the launch to explore the new observatory, and how it can help you keep up-to-date with the latest in digital policy. Book your e-seat [.](#)

responsible for the content they host, while allowing them to engage in good faith blocking of harmful content (Section 230 of the 1996 Communication Decency Act [\).](#) The order, which suggests that tech giants are politically biased, calls for the legislation to be clarified so that immunity from liability does not protect online platforms that 'engage in deceptive or pretextual actions stifling free and open debate by censoring certain viewpoints'. Any change in Section 230 that would lead to introducing liability for tech platforms could create major changes in the tech industry and the way the Internet is run.

President Trump's executive order has triggered a wide range of reactions. Critics note that placing more responsibility on social media companies for the content they host would in fact limit free speech, as the companies may be inclined to 'censor anything that might offend anyone' to avoid liability [.](#) The order is expected to be challenged in court.

Interestingly enough, Joe Biden, Trump's opponent in the next presidential elections, would also like to revoke Section 230, considering it to be an inadequate legal framework for the current Internet [.](#) Thus, the issue of liability of tech platforms will remain on the policy and regulatory agenda for years to come.

## 2. Contact tracing apps remain in focus

In our April newsletter, we mapped countries that had implemented or announced the implementation of contact tracing apps as a tool in fighting the spread

of COVID-19. When we published the newsletter on 4 May, there were 40 countries with digital tracing apps in place. Since then, the number has increased to 49.

Introducing digital tracing apps is not an easy task. It requires taking many considerations into account and winning the support of the population to use them – if their use is not mandatory. The main concern in using digital contact tracing apps is the protection of user data and privacy. One model of contact tracing apps is built on collecting user data and storing it in a centralised database managed by public authorities. Decentralised apps are based on bluetooth technology for proximity tracing and store the data only on the user’s device.

Privacy considerations have a direct impact on the efficiency of contact tracing apps, as users are more likely to use an app with higher privacy protections built in. Additionally, centralised apps raise concerns that the governments will keep tracing in place once the pandemic is over or use collected data for purposes other than preventing the spread of COVID-19.

The discussion over the use of centralised or decentralised apps has been particularly rich in Europe. The European Commission has stressed that tracing apps must be ‘voluntary, transparent, secure, interoperable and respect people’s privacy’, and the EU eHealth Network has issued guidelines for interoperability of contact tracing apps. Individual countries are taking different approaches. France and the United Kingdom are testing and evaluating centralised apps, while Germany, Switzerland and several other countries are opting for the decentralised approach based on the application programme interface (API) released by Apple and Google on 20 May.

### 3. Cyber-attacks get back to ‘normal’

Numerous cyber-attacks and data breaches were revealed in May. The European Parliament (EP) reported a data breach that exposed information of 1200 EP elected officials and staff, and 15 000 EU affairs professionals (including sensitive data and encrypted passwords). Europe’s largest private hospital network based in Germany and a company that facilitates payments on the UK electricity market were hit by ransomware attacks. EasyJet airline reported a cyber-attack that allowed hackers to access the travel data of 9 million customers (2200 of which also had their credit card details exposed).

Together with the new cyber-attacks, recent weeks also saw states issue new warnings, accusations,

and denials related to state-sponsored attacks. Australia called on states to adhere to the UN Group of Governmental Experts (UN GGE) Report of 2015, and refrain from engaging in or supporting cyber-activities that damage or impair health infrastructures. The USA declared that attacks against its energy grid constitute a national emergency. Germany charged a Russian hacker for a 2015 cyber-attack on the German Parliament, and connected him to the Russian military intelligence agency GRU; Russia denied any connection with the case. US authorities accused China of espionage about COVID-19 research; China denied the claims.

At the same time, the two UN processes that are called to address these concerns – the GGE and the Open Ended Working Group (OEWG) – were derailed due to the COVID-19 pandemics. In particular, the OEWG had to cancel its planned intersessional consultation, but has nevertheless continued collecting written submissions to the pre-draft of its report (with submissions by some 50 countries and dozens of companies and organisations, some of which have particularly focused on cyber-risks related to COVID-19). It remains to be seen if it will hold its final meeting in early July, as planned; its mandate might have to be extended, with more online consultations.

To boost the protection of the critical health sector, the CyberPeace Institute has issued ‘A Call to All Governments: Work Together Now to Stop Cyberattacks on the Healthcare Sector’, signed by many renowned figures from the public, private, and civil sectors (including several Nobel Peace Prize Laureates).

### Status of tracking apps



# Digital policy developments in May

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](https://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.



same relevance

## Global IG architecture

The first draft of the UN75 declaration stresses that the UN can act as a platform for 'shaping a shared vision on digital cooperation and addressing digital trust and security' issues.

The Global Forum on Cyber Expertise announced its Advisory Board for 2020–2022.



increasing relevance

## Sustainable development

UN agencies launched a Tech Access Partnership to scale up local production of critical health technologies.

The International Telecommunication Union (ITU) and the World Trade Organization (WTO) drew attention to digital divide challenges in the COVID-19 context.

African Union ICT ministers called for the rapid implementation of the African strategy for digital transformation. The UN Economic Commission for Africa cautioned that revamping Africa's telecoms infrastructure is crucial for digital health.

The ITU and the Broadband Foundation partnered to foster investment in south-eastern Europe's broadband infrastructure.

Ghana revealed policy initiatives to boost financial inclusion.



increasing relevance

## Security

The Council of the EU extended the cyber sanctions regime until 2021. Estonia passed a law for telecom network security reviews.

Many cyber-attacks were revealed, and new accusations and denials related to state-sponsored attacks emerged.

In two separate calls, Australia and international leaders asked states to refrain from and prevent cyber-attacks against the healthcare sector.

A Global Encryption Coalition was launched to promote and defend encryption.

Europol warned of a spike in the sexual abuse of children online.



same relevance

## E-commerce & Internet economy

G20 digital economy ministers committed to leveraging digital technologies in enabling economic recovery post-COVID-19.

The Organization for Economic Co-operation and Development (OECD) announced October 2020 as the new target date to reach global agreement on digital taxation. France reiterated plans to introduce a digital tax in 2020. Indonesia revealed a 10% value-added tax on Internet giants applicable from July.

Facebook announced Shops – a tool enabling businesses to set up online stores.



increasing relevance

## Digital rights

As countries continue to introduce COVID-19 contact tracing apps, privacy concerns remain in focus.

An Access Now report raised alarm over weak enforcement of the EU General Data Protection (GDPR).[Hungary suspended](#)[certain GDPR provisions.](#)

The Dutch Data Protection Authority launched an investigation into TikTok's child privacy practices.

Canada fined Facebook US\$6.5 million over misleading privacy claims.

The German data protection authority requested federal agencies not to use WhatsApp amid privacy concerns.

European Digital Rights called for a ban on biometric surveillance in the EU.



increasing relevance

## Jurisdiction & legal issues

France adopted a new law to combat online hate speech and other forms of harmful content. Twitter was taken to court in France over arguably insufficient measures to fight hate speech.

In the USA, the President issued an Executive Order on Preventing Online Censorship. The Court of Appeal dismissed a lawsuit claiming that tech companies suppress conservative views.

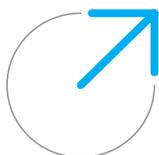
The US Supreme Court rejected a lawsuit against Facebook over responsibility for terrorist content.

Germany's Constitutional Court ruled that the right to privacy extends to foreign Internet users.

California's attorney general sued Uber and Lyft over classifying drivers as independent contractors.

Facebook announced an oversight board to 'exercise independent judgment' over certain content policy decisions.

The UN launched the Verified initiative to address COVID-19 misinformation through 'digital first responders'.



increasing relevance

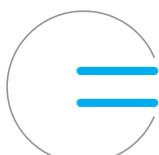
## Infrastructure

The USA imposed new trade sanctions on Huawei, affecting the company's chips supply. It also extended a temporary licence allowing US companies to continue doing business with Huawei until August.

Facebook announced plans to build a subsea cable for improving connectivity in Africa.

The European Commission urged member states not to delay 5G plans.

The .org controversy seems to have come to a halt.



same relevance

## New technologies (IoT, AI, etc.)

China launched communications satellites for Internet of Things (IoT) projects.

The European Parliament's Legal Affairs Committee started discussions on three draft reports on artificial intelligence (AI).

Microsoft announced an AI supercomputer.

Finland announced plans to develop its first quantum computer.

# Tech geopolitics: USA, China, and Huawei

Technology has played an important role in the geopolitical relations between the USA and China, which have unfolded on a strategic and tactical level. New dimensions of this tech geopolitics were revealed in May, as the US administration outlined its strategic approach towards China, while also imposing new trade sanctions on Chinese tech companies.

## From co-operation to competition

In a recently released 'United States Strategic Approach to The People's Republic of China' document, the White House points to a significant shift in US policy towards China. If initially the USA took a co-operation-based approach targeted at 'deepening [the] engagement' between the two countries, this is now shifting to a more competitive approach.

The USA notes that this change is 'based on a clear-eyed assessment of China's intentions and actions, a reappraisal of the United States's many strategic advantages and shortfalls, and a tolerance of greater bilateral friction'. It underlines, however, that competition should not lead to conflict and that co-operation is still welcome where Chinese and US interests align.

With the USA aiming to 'prevail in strategic competition with China', technology is inevitably an important component of the new strategic approach. In the document, the USA accuses China of using unfair practices to dominate the global information and communications technology (ICT) industry. It also makes reference to alleged frameworks of co-operation between companies like Huawei and ZTE and the Chinese security services which create 'security vulnerabilities for foreign countries and enterprises using Chinese vendors' equipment and services'.

## New trade sanctions

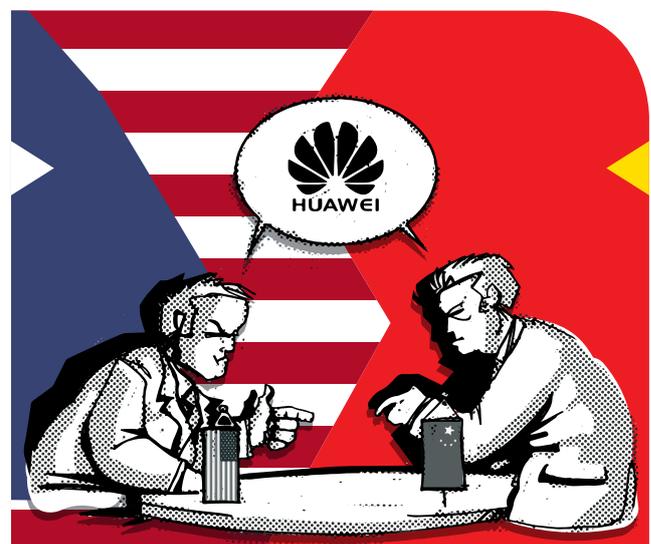
In its strategic document, the US administration notes that it will implement policies against the use of US technology to support China's 'technology-enabled authoritarianism'.

Such policies are already in place, with Huawei being the main target. In May last year, President Trump issued an executive order which banned US tech companies from selling their technologies to Huawei (including advanced computer chips essential for Huawei). Since then, a temporary licence (extended several times) has allowed US companies to still do business with Huawei. A new extension of this licence was announced in May and it is valid until August; it is, however, expected to be the last such extension.

The White House's attempts to reduce the presence of the Chinese tech industry in the USA took another dimension with a new executive order imposing additional trade sanctions that affect Huawei. The previous policy of banning the sale of advanced chips and chip designs to Huawei has been bypassed by various subsidiaries out of reach of US authorities. Now, the new sanctions mean that, when foreign companies that manufacture semiconductors use US technology during the production process, they must obtain export licences from US authorities before being able to sell their final products to Huawei. This affects the suppliers of technology (e.g. design, processes) for producing chips which are mainly part of the US companies' chip supply.

Experts are still grasping the implications of this new order for Huawei, the US industry, and the global industry. A recent article in *The Economist* notes that it may be difficult to enforce the order as envisioned (because the chipmaking tools industry is globalised and it is not so easy to determine what counts as US jurisdiction). At the same time, the order may also have the unintended consequence of 'driving a portion of America's chipmaking industry from its shores'.

Meanwhile, China has called on the USA to stop the 'unreasonable suppression' of Chinese companies and noted that it was ready to retaliate with counter-measures targeting US companies.



# Is the .org controversy over?

Since 2003, .org has been managed by the Public Interest Registry (PIR), a nonprofit subsidiary of the Internet Society (ISOC). In November 2019, ISOC announced its intention to sell PIR to equity firm Ethos Capital, generating considerable controversy. The recent decision of the Internet Corporation for Assigned Names and Numbers (ICANN) to reject the sale led to diverse reactions and open questions.

## ICANN's rejection of the .org sale

The ICANN Board had to consider multiple and divergent points of view and interests. Some saw the deal as an opportunity for PIR to become a for-profit entity able to reinvest in its operations, while others were concerned that a privatised PIR would no longer uphold the interests of the .org community.

In the end, ICANN decided (although not unanimously) that the 'the public interest is better served in withholding consent as a result of various factors that created unacceptable uncertainty over the future of the largest gTLD registry'. Reasons for this decision included, among others, lack of transparency about the investors involved in the proposed transaction, a concern that PIR could be 'drained of its financial resources', and doubts over how PIR would continue to serve the .org community.

## Main reactions to ICANN's decision

ISOC, PIR, and Ethos expressed their disappointment with the decision, stressing that the .org sale would have been good for all parties involved, including the .org registrants.

Critics of the deal saw the rejection of the sale as a win for the .org community and for the public interest. Organisations behind the SaveDotOrg coalition noted that a for-profit PIR would have been more inclined to 'serve the interests of its corporate stakeholders, not the nonprofit world' and that the sale would have put the reliability and security of .org at risk.

Others qualified ICANN's decision as a missed opportunity to improve the governance of .org. The Public Interest Commitments (PICs) proposed by Ethos would have brought in elements such as a Stewardship Council empowered to veto modifications to PIR's policies on issues such as censorship and the use of .org registrant data; annual transparency reports; and a commitment to not increase .org domain name fees by more than 10% per year on average for eight years. ICANN Board member Avri Doria noted that although these PICs could have been stronger, they would have protected the public interest better than the

status-quo. But there were also voices arguing that relying on the untested PIC would have been a risk.

## Open questions

**How much did the US juridical system influence ICANN's decision?** The Attorney General (AG) of the State of California (where ICANN is based) urged ICANN to reject the sale. While some saw the AG's intervention as beneficial, others expressed concerns: If the AG's request weighed significantly in ICANN's decision, does this create a dangerous precedent for future ICANN decisions on issues that may be even more controversial than the .org sale?

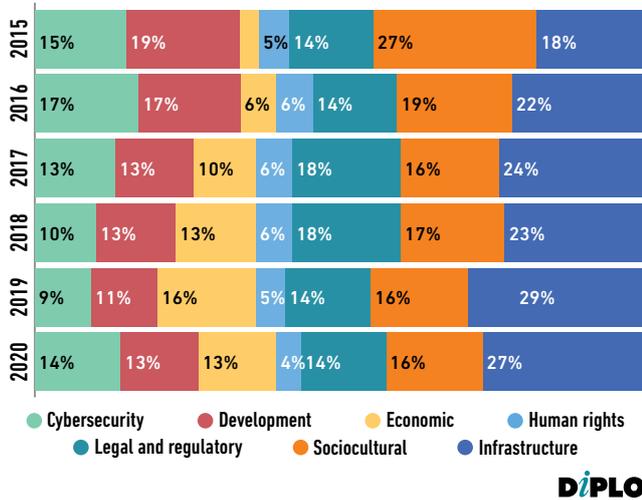
**Are there any ramifications of the decision into the broader domain industry?** ISOC, Ethos, and others argued that ICANN went beyond its mandate and acted as a regulator when it should have simply assessed whether a change of control for PIR would have affected the registry's operational and technical capabilities. Such a decision, they note, sets another dangerous precedent and risks 'suffocat[ing] innovation and deter[ring] future investment in the domain industry'. But there are also those who say that ICANN has simply acted in line with its responsibilities as outlined in the .org registry agreement.

**Is ISOC a proper home for PIR?** ISOC has been intensively scrutinised since it announced the proposed deal. Critics noted that the organisation should have consulted the community on the sale and that it could have put more effort into securing a proper management for .org after the transaction. Some go as far as arguing that ICANN should now put .org up for bid, questioning ISOC's ability to protect the public interest. But such a bid is unlikely to happen, and ISOC and PIR committed to making 'org even stronger'.

**Does ICANN's decision mean that the .org sale story is over?** It seems so, at least for the time being. ICANN left an open door for PIR to submit a new notice of change of control. But ISOC stressed that PIR is no longer for sale and that the registry will continue to operate in the current framework. In Ethos's view, 'the opportunity with PIR has passed'.



## Mapping of baskets



to gain new relevance, mostly due to the prominence of processes such as the GGE and the OEWG and the increase in cybercrime associated with the COVID-19 pandemic.

With regard to the human rights basket, it is noteworthy that over the years it remains the least represented category with its highest representation amounting to 6% and without any significant changes in value. Here, too, it is worth mentioning that individual human-rights-related topics – such as privacy – were prominently tackled in the context of related issues such as data governance or ethics.

## A closer look: the most prominent policy issues

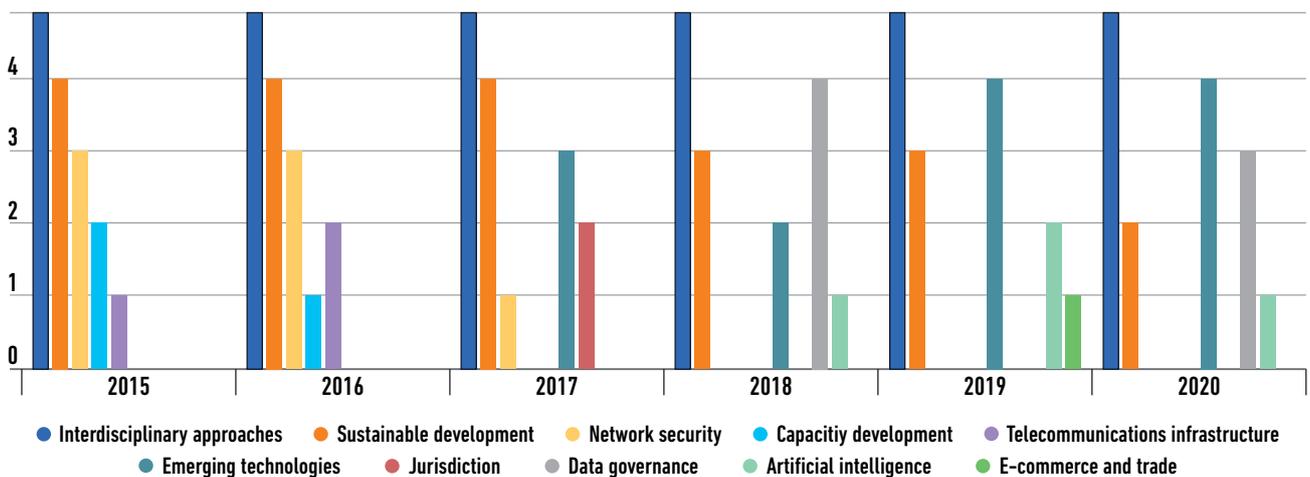
After analysing broader categories, we looked at individual issues for a more substantive grasp of the digital policy developments. The results offer a new perspective.

Online trust, ethical dilemmas, and multistakeholder governance of digital technologies – categorised under the issue of **interdisciplinary approaches** – were undoubtedly at the top of the international policy agenda as reflected in the newsletter. This coincides with the emergence of AI technologies, which triggered a global discussion on ethical frameworks. Trust, already a major issue for almost a decade, continued to be discussed in the context of security, privacy, and how we deal with data, culminating in the work of the UN High-level Panel on Digital Cooperation.

**Sustainable development** was the second most frequent issue from 2015 to 2017. In September 2015, governments renewed their commitment towards sustainable development by agreeing on an ambitious 15-year plan. Discussions on the sustainable development goals (SDGs) dwindled slightly in 2018, when a more prominent place was taken by debates on **data governance**.

In the past two years, **emerging technologies** refocused our attention on how data is used, generated, and shared. The spike in the coverage of emerging technologies also reflected the emergence of 5G, facial recognition, and robotics.

## Dominant issues by year



## Policy discussions in Geneva

Due to the COVID-19 crisis, no in situ events were held in May. However, Geneva-based organisations adjusted quickly and started delivering online events. The global focus on health and humanitarian issues has increased the relevance of Geneva dynamics for global governance. The following updates cover the main events of the month. For event reports, visit the Past Events section [on the Digital Watch observatory](#).

### ONLINE **AI for Good Global Summit** | weekly online events [↗](#)

Initially scheduled to be held in Geneva on 4–8 May, the ITU-organised AI for Good Global Summit was transformed into a continuous digital event [spread](#) across several months and including keynotes, expert webinars, project pitches, and interviews on AI-related issues. In May, the programme featured discussions on gender issues in AI, the role of AI in

tackling food insecurity, AI solutions for the environment, and combining crowdsourcing and AI to tackle the COVID-19 pandemic. Also included in the overall summit programme were meetings of the ITU Focus Group on AI for Autonomous and Assisted Driving and the ITU/World Health Organization Focus Group on AI for Health.

### ONLINE **Right On** | 6, 13, 20, 27 May 2020 [↗](#)

Held every Wednesday, the Right On series of online debates offers insights into human rights developments during the COVID-19 pandemic, but also goes beyond the current crisis situation. In May, the events addressed issues related to the use of technologies to facilitate contact tracing in response to the COVID-19 pandemic and related privacy challenges;

preventing COVID-19 from becoming a humanitarian disaster; whether lessons learnt from the pandemic could help build a more just, equitable, and peaceful world; and protecting the rights of older persons during the global health crisis.

[Read the summary reports.](#) 

### ONLINE **The Road to Bern via Geneva** | **Sharing data: Towards a data commons** | 26 May 2020 [↗](#)

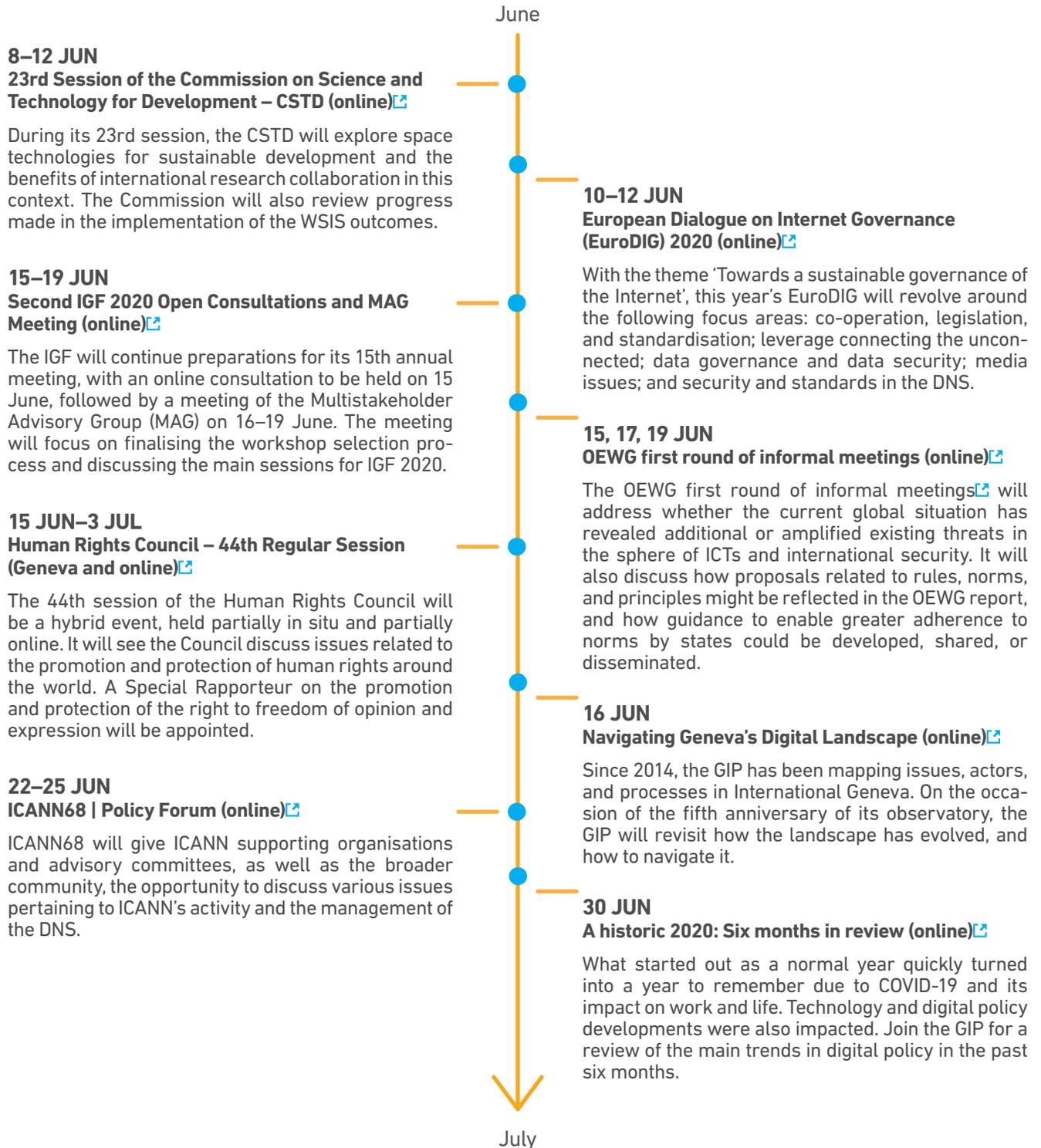
The *Road to Bern via Geneva* initiative [continued](#) with a third dialogue focused on data sharing, organised by the Permanent Mission of Switzerland to the UN in Geneva and the Geneva Internet Platform (GIP), and co-hosted by the European Organization for Nuclear Research (CERN) and the International Trade Centre (ITC). This and past and subsequent dialogues – on collecting, protecting, and using data [– will feed](#) into the 2020 UN World Data Summit (18–21 October, Bern). [Discussions](#) revolved around the benefits and risks of sharing and not sharing data; win-win solutions for data sharing; open data policies; and a ‘data commons’ and what is required from international organisations,

governments, businesses, and other stakeholders to implement this concept. Participants noted that sharing and developing a data commons with clear co-operation rules means more prosperity for all. But actors first need to consider which data categories they want to share, and on which level of processing. Incentives for sharing data might need to be designed by taking into account the types of challenges that various actors are facing. Actors also have to take into account what they want to do with the data, because they should not create additional data graveyards.

[Read the summary reports.](#) 

# The main global digital policy events in June

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 details and for the proceedings of some events – including reports from individual sessions and a final report summarising the discussions – please check in regularly at the *Digital Watch* observatory.



## Future of meetings

On 12 May, we hosted an online conference on the Future of meetings. [The main discussion](#) focused on the interplay between onsite and online meetings, and the emerging form of hybrid meetings. Here are the main takeaways.

### **Plan! Prepare! Practise!**

When holding online events, organisers need to spend time planning, preparing, and practising to ensure that everything runs smoothly from a technical perspective and in facilitating discussions and interactions.

### **Inclusion: Amplifying weak voices through e-participation**

Online meetings offer new possibilities for including quieter voices in global policymaking, that is, those who may have been left behind in traditional meetings. This can be particularly relevant for small and developing countries, marginalised groups, and people with disabilities.

### **Ensuring cognitive consonance: Avoiding spaghetti meetings**

Maintaining focus during online conferences is challenging. Organisers need to put participants in control of their online experience and ensure they have a cognitive grasp of the event without necessarily knowing all the details.

### **Some things stay the same: The devil is in the detail**

Organising an online event opens the possibility of many unknowns. Dealing with them requires a flexible mindset to react creatively and quickly to crisis situations, and empathy for online participants when dealing with unforeseen circumstances.

### **The old and the new: Navigating between tradition and innovation**

While diplomatic procedures need to adapt to new online dynamics, many elements of traditional diplomatic protocol will remain relevant, such as precedence, equality, order to statements, and voting.

### **Priorities: Moving beyond technology**

An online event is not only about technology. Organisers should not overlook essential issues such as good moderation and an understanding of social, emotional, and policy contexts, which are relevant for every e-meeting.

**For a more in-depth summary of the discussions and links to video recordings, visit the [conference website](#).**

#### About this issue

Issue no. 50 of the *Digital Watch* newsletter, published on 1 June 2020 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđelković, Stephanie Borg Psaila, Andrijana Gavrilović, Tereza Horejsova, Pavlina Ittelson, Djordje Jančić, Jovan Kurbalija, Nataša Perućica, Vladimir Radunović, Sorina Teleanu | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo's CreativeLab. | Get in touch: [digitalwatch@diplomacy.edu](mailto:digitalwatch@diplomacy.edu)

#### Go deeper with more resources

Wherever you see the blue icon  click on it in the digital version to access the source or additional resources.

#### On the cover

*Celebrating 50 issues of timely updates on digital policy.* Credit: Vladimir Veljasević

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

