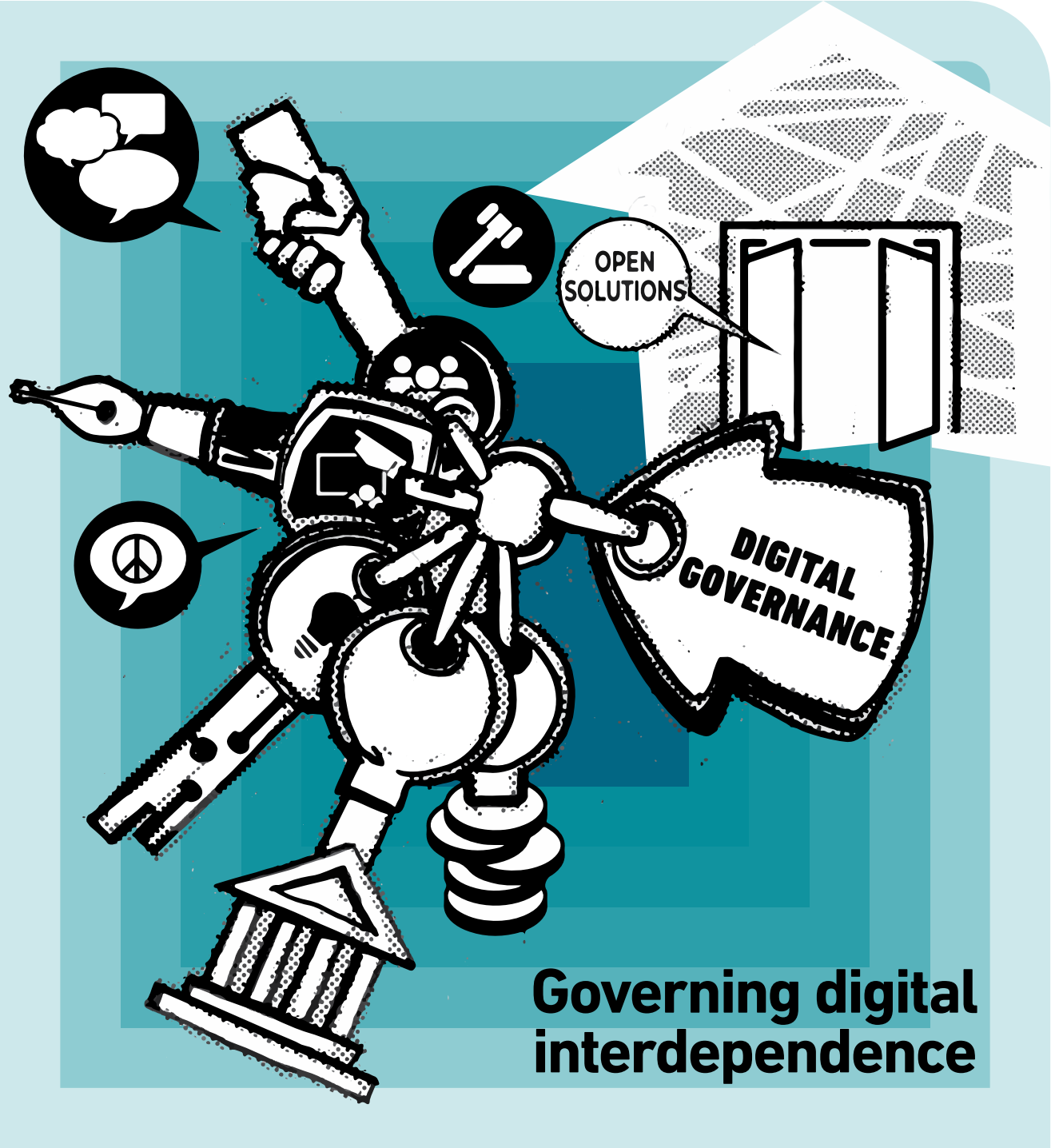
Geneva Internet Platform
DigitalWatch
dig.watch

Issue 55, November 2020
Newsletter



Governing digital interdependence

TRENDS

Calls to tackle terrorist content online intensify, more antitrust actions emerge against tech companies, and facial recognition is in the spotlight.

Pages 2–3

CYBER-NORMS

The UN General Assembly First Committee adopted competing resolutions on cyberspace and international security.

Pages 7

IGF TRENDS

Our data analysis reveals how IGF discussions have evolved over the past three years and what issues gained and lost prominence.

Pages 8–9

GENEVA DIGITAL ATLAS

The Geneva Internet Platform launched a comprehensive mapping of the digital policy and Internet governance scene in International Geneva.

Page 12

The top digital policy trends in November

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

1. Tackling terrorist content online

In light of recent terrorist attacks across Europe, tackling the spread of terrorist and extremist content online has come into sharper focus. In a joint statement issued on 13 November, EU home affairs ministers expressed their intention to finalise negotiations on the regulation on terrorist content online by the end of the year. The regulation would enable competent authorities in one EU member state to issue content removal orders with cross-border effect, requiring hosting service providers to remove content or disable access to it in all member states within an hour or less of it being reported.

The regulation, proposed in 2018, is now being negotiated between EU institutions. One major area of contention is related to whether cross-border removal orders should have direct effect or whether they need to be confirmed by authorities in the host country. Some parties to the negotiations argue that such a confirmation is needed to ensure that the rule of law and human rights frameworks in the host country are upheld; others claim that the procedure would defeat the whole purpose of a cross-border order and delay the removal of content.

Beyond the disagreement between the negotiating parties, the regulation has also generated human rights concerns. Several civil society groups, the Special Rapporteur on the promotion and protection of the right to freedom of expression, and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism have noted that the proposed definition of terrorist content is broad and may unproportionally limit freedom of expression and access to information. Other concerns relate to a lack of judicial review and effective appeal mechanisms for removal orders, and the risk that Internet companies may decide to pre-emptively remove content that is lawful or develop automated tools for content removal that could result in over-censorship.

The need to tackle terrorist content online has also sparked new debates on facilitating the access of law enforcement agencies (LEAs) to encrypted digital evidence. In their joint statement, EU home affairs ministers called on the European Council to 'consider the matter of data encryption so that digital evidence can be lawfully collected and used by the competent authorities while maintaining the trustworthiness of the products and services based on encryption technology'. In this vein, a leaked draft Council resolution on encryption reiterates strong support for encryption, but also requires enabling LEAs to access content in a readable and usable format where authorisation is lawfully issued.

This position is somewhat similar to the statement issued in October by the UK, the USA, Australia, New Zealand, Canada, India, and Japan, which underlines support for encryption, but invites companies to actively cooperate with states to find ways to allow LEAs to access encrypted evidence. The technical community cautions that such access is not possible without weakening encryption, while civil society organisations warn about the potential human rights implications of such actions.

2. More antitrust action against tech companies worldwide

Governments around the globe are trying to curb the power of big tech via antitrust proceedings. In October, the US Congress unveiled an antitrust report about Amazon, Apple, Facebook, and Google stating that each of them is holding monopoly power and that parts of their businesses should be broken up. Similar accusations are trending elsewhere, too.

One of the unfair competition issues analysed by authorities is related to tech companies prioritising their own products and services over those of competitors. The European Commission has recently filed antitrust charges against Amazon, claiming that the company has unfairly used marketplace sellers' data to harm their businesses. The Commission believes Amazon harvests non-public data from sellers who use its services, identifies popular products, and then sells similar products at lower prices. The European Commission also launched an investigation into Amazon's 'buy box' tool, to determine whether the company is giving preference to its own products.

Google, which in October was hit with a major antitrust case in the USA, is again under fire in Europe.

A group of 165 companies and industry bodies filed a complaint to the European Commission seeking harder antitrust enforcement against Google for giving preferential treatment to their own products and services. Meanwhile, the UK is considering opening a competition inquiry into Google for dominance in online platform marketing and advertising, following a complaint that the launch of so-called Privacy Sandbox technology would put advertising under Google's control. The country has also announced plans to introduce a statutory code of conduct to govern the market behaviour of online platforms.

Google has also attracted the attention of the Indian Competition Commission, which opened antitrust proceedings against the company for the alleged abuse of its dominant position in the payment services market. The body is investigating claims that Google is using its Play Store to promote its own payment service, Google Pay.

In China, the antitrust authority has released draft rules against anti-competitive behaviour. Targeted mostly at major Chinese tech companies, like Alibaba and Tencent, the proposed rules would prohibit companies from sharing consumer data and attempting to stifle smaller competitors. They would also no longer be able to force third-parties into exclusive arrangements, or treat customers differently based on their data and spending habits.

These actions demonstrate an increased appetite among competition authorities to scrutinise big tech and their behaviour towards competitors and customers. It remains to be seen whether this will lead to significant changes in how major companies operate.

3. Facial recognition in the spotlight

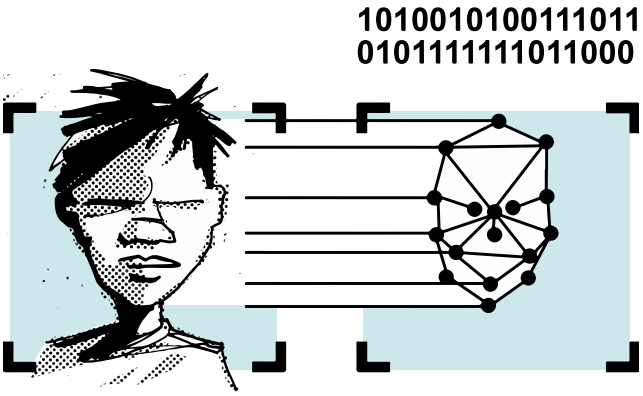
Concerns about the implications of facial recognition technology (FRT) are not new. Several studies have shown that the technology presents significant bias and discrimination risks, and poses threats to individuals' right to privacy. And while some authorities have moved to ban the use of FRT, in particular by LEAs, the debate on whether and how the technology can be used safely is far from over.

In Europe, several civil society groups concerned about the increased use of FRT in public spaces have launched the Reclaim Your Face campaign calling for transparency from authorities and companies about the use of such technologies. They also call for a ban on biometric mass surveillance, which could negatively affect people's rights and freedoms.

In the USA, citizens of Portland, Maine have voted in support of a ballot initiative to ban the use of facial recognition by LEAs and other city agencies. The measure is not the first of its kind: several other cities have introduced such bans (examples include Boston, San Francisco, and Sommerville). In a different move, the Los Angeles Police Department banned the use of third-party facial recognition systems, after it was revealed that several detectives had used the Clearview AI platform without permission. The LA police can only use a system maintained by local authorities, which compares images input by the police against images of booked criminals (unlike Clearview AI, which compares images against millions of photos available online).

Is banning the use of FRT the most appropriate solution? Tech companies tend to favour regulations over outright bans. Microsoft has recently reiterated its call for regulations that put in place safeguards for FRT use. IBM has expressed its readiness to work with US authorities to 'prohibit the use or export of facial recognition for mass surveillance, racial profiling, or violations of basic human rights and freedoms'.

Earlier this month, the Freedom Online Coalition called on states to refrain from using FRT and other artificial intelligence (AI) systems for repressive and authoritarian purposes. The 32 countries that form the coalition have also asked for international multistakeholder cooperation in the development of norms, rules, and standards to guarantee that AI systems are developed, used, and governed in line with international human rights law.



Digital policy developments in November

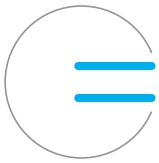
The digital policy landscape is filled with new initiatives, evolving regulatory frameworks, and new legislation and court judgements. In the *Digital Watch* observatory – available at **dig.watch** – we decode, contextualise, and analyse ongoing developments, offering a digestible yet authoritative update on the complex world of digital policy. The monthly barometer tracks and compares the issues to reveal new trends and to put them into context with 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 at the observatory.

increasing relevance

Global IG architecture

The 15th Internet Governance Forum concluded with a call for global unity to bridge digital divides.

The World Internet Conference called for an approach to global cyberspace governance 'which is based on extensive consultation, joint contribution and shared benefits'.



same relevance

Sustainable development

The UN Technology Bank and the Commonwealth launched a partnership to build science, technology, and innovation capacity for least developed countries.

The International Telecommunication Union (ITU) and Norway partnered to support Ghana's Digital Transformation Centres initiative.

Australia launched a public consultation on a draft digital identity legislation. Nigeria approved a digital identity policy for internally displaced persons.

The ITU's *Measuring Digital Development: Facts and figures 2020* report highlighted persistent connectivity gaps in rural areas.

increasing relevance

Security

The UK revealed its National Cyber Force. Canada named 'state sponsored programs of China, Russia, Iran, and North Korea' as strategic threats.

The UN General Assembly (UNGA) First Committee adopted competing resolutions on cyberspace and international security. EU member states plan to speed up the finalisation of the regulation on terrorist content online. An EU draft resolution supports 'security through encryption' and 'security despite encryption'.

increasing relevance

E-commerce & Internet economy

The World Trade Organization's *World Trade Report 2020* noted that countries are increasingly adopting policies in support of digital innovation. The Organisation for Economic Co-operation and Development (OECD) released its *Digital Economy Outlook 2020*, analysing trends, opportunities, and challenges in the digital economy.

China presented draft rules to curb anti-competitive behaviour by tech companies. The UK announced plans for a new competition regime for tech giants.

France expects tech companies to pay the digital services tax starting December 2020. Canada intends to start levying digital sales taxes.

WhatsApp launched mobile payments in India.

Fifteen Asia-Pacific countries signed a partnership to facilitate international trade.

Digital rights

same relevance

Apple faces privacy complaints in Europe over ID generated by iPhones.

The European Commission published draft standard contractual clauses for transferring personal data to third countries.

The Canadian government proposed stronger data protection rules.

The Committee on the Elimination of Discrimination against Women called for a crack-down on trafficking of women and girls in the digital age.

Facebook and Google extended bans on political advertisement in the USA. Facebook, Twitter, TikTok, and YouTube took measures to contain the spread of misinformation about US election results.

Jurisdiction & legal issues

increasing relevance

The European Commission published a proposal for a data governance regulation.

TikTok's owner ByteDance filed a petition against the US President's executive order that required the company to divest its US assets by 12 November 2020. The Committee on Foreign Investment in the USA extended the divestiture deadline until 4 December. The US government appealed a court decision which blocked the TikTok ban from coming into force on 12 November.

Turkey fined major Internet platforms for not appointing official representatives in the country.

The Austrian Supreme Court ordered Facebook to delete all defamatory statements globally concerning a politician.

India banned 43 mobile apps from being used on its territory.

Facebook and Twitter testified in the US Senate on platform responsibility.

Infrastructure

decreasing relevance

Alphabet's Project Taara is working with partners in Kenya to deliver high-speed connectivity via beams of light.

Huawei filed an appeal against the Swedish telecom regulator's decision to exclude the company from 5G networks. In the UK, telecom companies will not be allowed to install new 5G equipment from Huawei after September 2021.

New technologies (IoT, AI, etc.)

same relevance

The Freedom Online Coalition released a statement on AI and human rights. The Privacy Commissioner of Canada issued proposals for regulating AI. The US White House published guidance for regulating AI applications. Brazil announced a national AI innovation network.

European NGOs launched a campaign against FRT in public spaces. Citizens of Portland City, USA voted to ban the use of FRT by city agencies.

The EU Agency for Cybersecurity published guidelines for securing the Internet of Things (IoT) supply chain. The US Senate passed the IoT Cybersecurity Improvement Act.

Governing digital interdependence

As the search for digital governance solutions accelerates, the debate galvanises around some key issues: Do we need a digital home for humanity where countries, companies, and citizens can address their digital issues? Are issues such as protection of data and cybersecurity ripe for a grand tech bargain? What roles should governments and businesses have in the future digital governance?

While answers to these and other questions are very diverse, there is growing consensus worldwide that something needs to be done on global digital governance to prevent the disintegration of the Internet and ensure its future as an enabler of social and economic progress worldwide. Three initiatives have been in focus recently.

1. **Internet Governance Forum Plus (IGF+)** is the most advanced proposal for digital governance. The building blocks for IGF+ are outlined in the UN Secretary-General's Roadmap for Digital Cooperation (June 2020). Moreover, Considering the Tunis Agenda, the Secretary-General has a formal mandate to implement the IGF+ proposal.

Building on the IGF's wealth of experience and expertise, the IGF+ architecture would include the following main upgrades:

- Leadership: a strategic and empowered multistakeholder high-level body to strengthen links between IGF deliberations and other decision-making spaces including parliaments, business associations, and international organisations.
- Inclusion and capacity building: a network of help desks to increase inclusion and assist small and developing countries to participate meaningfully in digital policy-making.
- Cooperation: functional links created with governance and policy spaces where digital policy issues are addressed from local to global level, including linkages among the UN organisations.

2. A **Technology Alliance**, proposed by the Center for New American Security focuses on dealing with China's fast digital growth. It argues for a 'selective decoupling from China and a shift to managed interdependence'.

The Alliance would start as a club of 10 like-minded countries: Australia, Canada, France, Germany, Italy, Japan, the Netherlands, South Korea, the UK, and the USA. The EU would join as a non-voting member. A modest expansion of membership is envisaged, including the participation of India. Decisions would be made by consensus among governments and certain levels of multistakeholder participation would inform alliance decisions and actions.

Priority focus: secure and diverse supply chains, international standards-setting, critical technology protection, multilateral export control of cybersecurity technologies, new investment mechanisms for secure digital infrastructure, and common norms on cyber issues.

3. A **Digital Trade Zone** to Promote Online Freedom and Cybersecurity, proposed by the Council of Foreign Relations, intends 'to form a digital trade zone that ties the adoption of democratic values online to access to digital markets'. It aims to 'weaponize digital trade relations' by allowing digital trade with China and other countries on the condition that they respect rules on cybersecurity, human rights, and core values of democratic societies.

The digital trade zone would be established by treaty-based organisations, with a leading role for governments and some participation by the tech industry and Internet users groups. Priority focus: expansion of rules on intellectual property, anti-spam, theft of trade secrets; immunity of cloud companies from legal liability for user-generated content; prohibition of governments to condition market access to request for source code; free flow of digital trade across borders; ban of data localisation; notification system for cyber malicious activities; prohibition of electronic spying among members of the zone (only human intelligence will be allowed); and ban of covert election interference.

Governing digital interdependence is at the core of the three proposals. IGF+ is about harnessing this interdependence via a global arrangement. The Technological Alliance focuses on managing interdependence in supply chains, digital trade, and cybersecurity. The Digital Trade Zone builds on 'weaponizing' interdependence by leveraging access to digital markets.

For a long time, interdependence has contributed to digital goods, from economic growth to societal progress. However, the same networks are used for 'digital bads', from cybercrime to fraud and cyber-attacks. Ultimately, countries, companies, and citizens will have to find a trade-off between the beneficial and endangering aspects of digital interdependence. These trade-offs will shape the governance of digital interdependence in the coming years.

The parallel roads of cybersecurity within the UN

The UNGA First Committee adopted two competing resolutions on the future of the Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security, and the Open-Ended Working Group on developments in the field of ICTs in the context of international security (OEWG). Many have pointed out parallels with the not so distant past, when in 2018 two resolutions on creating OEWG and renewing GGE were approved.

The underlying tensions between the USA and its allies on one side and Russia and China on the other were still evident towards the end of GGE and OEWG processes, this time in resolutions on how the two tracks should proceed at the expiration of their mandates. The deadline for the OEWG to present a consensus report to the UNGA was extended to after its third and final session, scheduled for 8–12 March 2021. The GGE is to present its final report to the UNGA on 14–21 September 2021. Even before this work is concluded, two ways forward have already been approved by the UNGA First Committee.

Resolution A/C.1/75/L.4 (USA and Western allies)

The First Committee approved a resolution put forward by the USA and its allies that calls on states to wait until the current GGE and OEWG meetings are completed and their outcomes considered by the UNGA (i.e., autumn 2021). The UNGA should then decide on any future work, as needed.

The resolution invites states to provide views on cybersecurity efforts at the national level, and their understanding of the key concepts mentioned in previous GGE reports. It also notes that the dissemination and use of information technologies affect the interests of the entire international community, and that 'optimum effectiveness is enhanced by broad international cooperation'.

Resolution A/C.1/75/L.8 (Russia, China, and others)

The second approved resolution, put forward by Russia, renews the OEWG for a period of five years – 2021 to 2025 – with the same mandate. The new OEWG starts its activities when the work of the current OEWG concludes, and considers its outcomes. The resolution mandates that the organisational session of the new OEWG be held in 2021 and includes the establishment of thematic subgroups, allowing interaction with other stakeholders. In addition to an annual progress report, the group is to provide a final report to the 80th UNGA, starting in autumn 2025.

This resolution puts the combatting of the dissemination of false or distorted news firmly within the state's sovereignty and considers that such behaviour could count as interference in the internal affairs of a state. It further recognises the duty of states to abstain from 'any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other states'.

The US-sponsored resolution was adopted with 153 votes in favour, while the Russian-sponsored one was adopted with 104 votes: several countries voted for both, despite their somewhat conflicting nature. This may signal confusion, or a hesitancy to take sides in this geopolitical split.

Programme of Action (France, Egypt, and others)

The adoption of the two competing resolutions leaves the Programme of Action (PoA), supported by the EU and 40 countries (including all African Union (AU) states), in a difficult position. While it had wide support in the last round of OEWG deliberations, it seeks to replace the dual-track discussions of the GGE/OEWG with a single, permanent UN forum, which is now contrary to the adopted resolutions (more on the PoA in our October 2020 newsletter). The PoA has, however, not been proposed as a resolution but rather as a possible recommendation in both reports.

It is interesting to note that France, AU countries, and non-EU countries that supported the PoA did not support the resolution put forward by the USA. On the other hand, the majority of EU member states supported both the PoA and the US resolution, bringing the number of countries supporting both proposals to 34.

What comes next?

While the First Committee has adopted the two resolutions, they still need to be approved by the UNGA. Follow our dedicated page on the *Digital Watch* for updates on both processes.

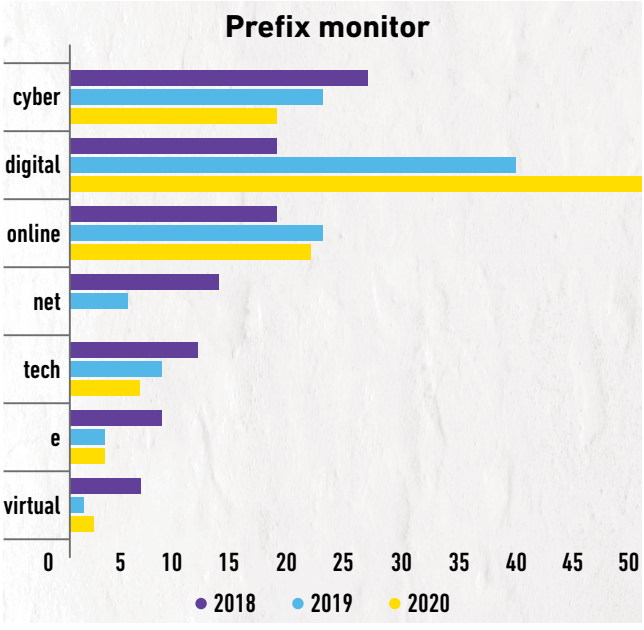
Digital policy trends at the IGF: A look at the past three years

This year, the annual IGF meeting was convened completely online. Within a different format, stakeholders got together to explore some of the most pressing digital policy issues. In our IGF 2020 report, we provide a thematic summary of the debates. To see how IGF discussions have evolved in recent years, we conducted a comparative data study of IGF 2018, IGF 2019, and IGF 2020.

Digital in the spotlight

Prefixes oftentimes point to the emergence of new developments in the tech field. Moreover, they are indicative of how actors frame policy narratives. For the past three IGFs, we have tracked the use of six prefixes: cyber, digital, online, virtual, tech, and e.

The most significant change between 2018 and 2020 is the noticeable rise in the use of the term *digital*. From a second place in 2018 (shared with *online*) with a frequency of 18% (in comparison to other prefixes), the prefix *digital* has since held the first position with an occurrence of 39% and 50%. One of the reasons behind its growth is that discussions have been extended beyond Internet-only issues to encompass the broader digital sphere. For instance, efforts to expand Internet access are now discussed in the context of digital inclusion, while digital trust is discussed not only in relation to Internet services, but also in the framework of other technologies such as AI. The rise in the use of *digital* over the past two years is also linked with the emergence of the term *digital cooperation*, following the High-level Panel on Digital Cooperation and the UN Secretary-General's Roadmap for Digital Cooperation.



Despite the prominence of cyber-related topics on the IGF agenda, the slow yet evident decline of the term *cyber* is another development that has been observed in the last three years. From first place in 2018, when a number of sessions were dedicated to cybercrime, cybersecurity, and cyberbullying, cyber moved down to the third spot in 2020. A similar trend is noticeable for prefixes *tech* and *e* whose use decreased from 11% and 8% in 2018, to 8% and 3% in 2020, respectively.

Issues and baskets: something old, something new

To determine whether and how the focus of IGF discussions has changed over the past three years, we took a close look at the session transcripts to identify the most prominent topics they tackled. Our analysis relied on *Digital Watch*'s taxonomy of digital policy; we went beyond the appartenance of each session to the thematic tracks that the IGF introduced in 2019.

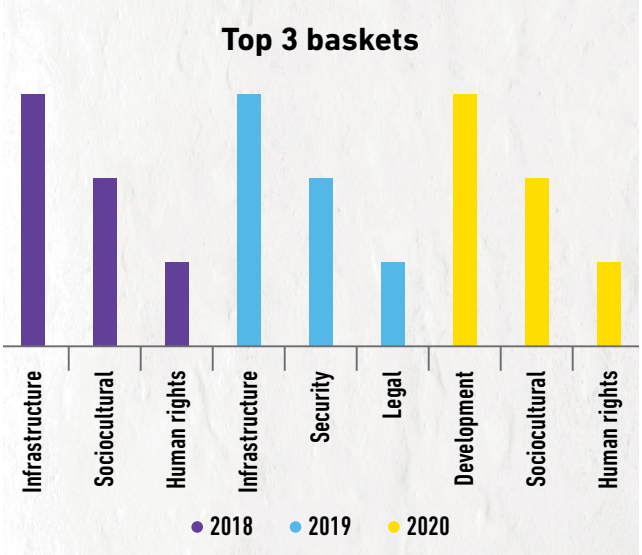
The past three years saw some constants and some changes in the rank of the most prominent digital policy issues. The high visibility of interdisciplinary approaches is perhaps the most obvious example. Focusing on questions of trust, ethics, and governance, this issue was the only one featuring among the top three issues in all three years, navigating from second place in 2018 to first in 2019 and ultimately third in 2020.

Occupying third place in 2018, content policy gained more visibility this year, moving to second position. This reflects the growing attention paid over the past year to issues such as misinformation and disinformation in the context of both COVID-19 and elections, along with the intensification of debates on the liability regime for Internet platforms with regard to the content they host.

Sustainable development was undoubtedly the most prominent issue in 2020. This was discussed in relation to the COVID-19 pandemic, which has emphasised digital inequalities around the world and the need to advance digital inclusion as an essential step towards achieving sustainable development. The role of digital technologies in advancing economic and social development was also a recurrent topic across multiple sessions.

Access and data governance only appeared once in the top three issues in the period 2018–2020. This does not necessarily mean that the issues lost relevance, but rather that they were less discussed as stand-alone topics, and more so at the intersection with other issues. For instance, access was integrated into debates on sustainable development, while data governance was part of discussions on digital trust.

The distribution of dominant issues is to an extent reflected in the ranking of baskets. The infrastructure basket was the most prominent in 2018 and 2019 (with many discussions focusing on telecom infrastructures, critical Internet resources, and advanced technologies such as AI and the IoT), until it was substituted by development in 2020. In addition to sustainable development, other topics that led to the prominence of the development basket include capacity development and e-waste and other environmental issues (with environment being one of the IGF 2020's main tracks).



An interesting observation in 2020 is the return of the sociocultural and human rights baskets among the top three most prominent ones. Featuring at the top in 2018, these two baskets were replaced in 2019 by the cybersecurity and legal baskets. In 2020, the rising prominence of content policy and trust issues, together with a rather new emphasis on online education brought the sociocultural basket back into focus. If in 2019 human rights issues were tackled more holistically in debates on the impact of the Internet and other digital technologies on societies at large, they made it back to the top in 2020, as we saw more nuanced discussions on privacy and data protection, children's rights, gender rights, and the rights of persons with disabilities in the digital space.

Notably missing in our rankings of most prominent issues and baskets are economic topics. While issues such as e-commerce, the future of work, and inclusive digital economies were occasionally covered in discussions (mostly in relation to inclusion and sustainable development), economic topics tend not to be among the most important ones for the IGF community. This is despite the growing attention that topics such as taxation and competition are attracting at the international level.

The *Digital Watch* observatory provided just-in-time reporting from IGF 2020. Visit the dedicated space to access session reports, a mid-IGF report, and a final report summarising the discussions.

Policy discussions in Geneva

Numerous policy discussions are hosted by Geneva-based organisations every month. The following updates cover some of the main events in November.

Geneva Peace Week | 2–6 November 2020

Held online under the theme 'Rebuilding trust after disruption: Pathways to reset international cooperation', the conference included a track dedicated to cyberpeace. One session called for international efforts to stop the use of digital technologies as tools of violence and war. Another session discussed the need to build trust in cybermediation activities through cooperation between technology designers, providers, and users. Other debates looked at combating cyber operations against healthcare facilities, the opportunities and threats that social media brings to peacebuilding, and the urgency of taking action against violent narratives on the Internet.

Roundtable on Virtual Reality and Mediation | 5 November 2020

The event brought together virtual reality (VR) experts and humanitarian practitioners to discuss the potential of VR for peace mediation. The debates revealed that VR could be used before a negotiation (e.g. as a training tool for mediators and to raise awareness on conflict issues on the ground) and during the negotiation (e.g. to bring the perspective of civilians to the table). But the technology also comes with challenges (e.g. it could be too immersive and result in anxiety), so stakeholders need to carefully assess the context and potential uses before deploying it.

Water and Cybersecurity: Protection of Critical Water-related Infrastructure | 18 November 2020

Organised by the World Meteorological Organization (WMO), the online debate looked at how to increase the resilience of water sectors against cyber-attacks. Participants noted that partnerships with the tech industry are essential in better managing cyber-risks that threaten critical water infrastructures, and in developing prevention and mitigation capabilities. It was also argued that states need to clarify the level of protection that international law offers to water infrastructure during both peacetime and conflicts.

Data 2025 V.2.0 – Conference | 23 November 2020

Organised by the Graduate Institute of International and Development Studies and the Centre for Digital Trust, the online conference started with an overview of how (personal) data is used and misused in the digital space. The role of data in addressing the COVID-19 pandemic was also explored, with a focus on the need to protect sensitive data when using, for instance, contact tracing apps. A discussion on the principles of data governance underlined the importance of multistakeholder cooperation in fostering trust in the use of data.

Digital Security and Economic Recovery | 26 November 2020

Held as part of the Geneva Dialogue on Responsible Behaviour in Cyberspace, an initiative led by DiploFoundation and the Swiss Federal Department of Foreign Affairs, this online event gathered high-level officials of the Swiss government, UBS, Kaspersky, Huawei, Microsoft, and DiploFoundation in a discussion on the need to build trust and security in the digital economy as a condition for the world to truly benefit from the digital transformation processes accelerated by the COVID-19 pandemic. Participants discussed how the fragmented regulatory environment impacts the security of digital products and services, and called for more collaboration between the public and private sectors in reducing the vulnerabilities in cyberspace and facilitating financial and economic recovery through trusted digital technologies. The event built on a series of discussions among lead global companies, partners to the Geneva Dialogue, and on their good practices in embracing security by design, showcased in a draft output document open for comments.

The main global digital policy events in December and January

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 summary reports and digests from individual sessions – check in regularly at the *Digital Watch* observatory.

December

1–3 DECEMBER
OEWG fourth round of informal virtual meetings (online)

The OEWG will hold its fourth round of informal virtual meetings between 1 and 3 December 2020. The group will discuss the regular institutional dialogue section of its revised pre-draft report.

4–10 DECEMBER
Informal Multi-Stakeholder Virtual Dialogue Series on OEWG pre-draft (online)

Intended to complement the work of the OEWG, the dialogue series is an informal event organised by the multistakeholder community and a number of UN member states. It collects stakeholder perspectives on the OEWG's pre-draft report and creates opportunities for in-depth dialogue between states and NGOs on the six substantive issues for discussion enumerated in the Resolution establishing the OEWG: international law; existing and emerging threats; rules, norms, and principles; capacity building; regular institutional dialogue; and confidence-building measures (CBMs). A side event on gender approaches to cybersecurity will also be featured on the agenda.

25–29 JANUARY
The Davos Agenda (online)

Organised by the World Economic Forum (WEF), this week-long event will mark the launch of WEF's proposal to rebuild the economy sustainably following the COVID-19 pandemic: *The Great Reset*. Each day of the event will focus on one of the five domains of the initiative: designing cohesive, sustainable, and resilient economic systems; driving responsible industry transformation and growth; enhancing stewardship of global commons; harnessing the technologies of the Fourth Industrial Revolution; and advancing global and regional cooperation. The event will also mark the start of preparations for the Special Annual Meeting, which has been postponed from January, when it is traditionally held, to spring 2021.

4 DECEMBER
The Future of Work Summit (online)

The second summit will be held as a launch event for the Thinking Ahead on Societal Change (TASC) platform, an open forum on universal challenges supported by the Government of Switzerland. It will focus on three areas of change: working on the frontline, working online, and working in radical uncertainty.

14–18 DECEMBER
GGE third session (online)

The sixth GGE will hold its third substantive session on 14–18 December. The GGE's remit is to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, and how international law applies to the use of ICT by states, as well as norms, rules, and principles of responsible behaviour of states, CBMs, and capacity building.

28 JANUARY
Geneva Blockchain Congress (online)

The third Geneva Blockchain Congress will once again address the theme 'from laboratory to market via ethics, regulation, and governance'; returns on investment (ROIs); and use cases. The programme will focus on eight fields of activity: public administration, deep tech evolution; banking and finance, regulation and legal framework, illicit trade and counterfeiting, health and wellbeing, supply chain and logistics, and social and humanitarian applications.

February

Geneva Digital Atlas

On 30 November, the Geneva Internet Platform (GIP) launched the Geneva Digital Atlas, a comprehensive mapping of the digital policy and Internet governance scene in International Geneva.

More than 50% of Internet and digital policy issues are addressed by Geneva-based organisations. The Atlas maps this complex scene, providing an in-depth coverage of the activities of more than 40 actors, including an analysis of policy processes and a catalogue of core instruments and featured events. Its goal is to connect policy dots among a wide range of processes and organisations dealing with issues related to data, AI, cybersecurity, e-commerce, and privacy, among others.

By using the Atlas, digital policy professionals and any other interested stakeholders can:

- Delve into the digital policy work of each organisation and their relevance for the 2030 Agenda for Sustainable Development.
- Identify convergences, similarities, and gaps in the digital work of organisations in International Geneva.
- Consult a repository of the main instruments (policy documents, resolutions, and declarations) that each organisation has adopted in addressing digital issues.

The Geneva Digital Atlas builds on 20 years of research, training, and policy-shaping work by the GIP and DiploFoundation. It is a living document, constantly updated via the *Digital Watch*.

Explore it at **dig.watch/actors/geneva**.

About this issue
Issue no. 55 of the *Digital Watch* newsletter, published on 1 December 2020 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđelković, Andrijana Gavrilović, Pavlina Ittelson, Jovan Kurbalija, Marco Lotti, Nataša Perućica, Sorina Teleanu | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo's CreativeLab. | Get in touch: 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
Governing digital interdependence. Credit: Vladimir Veljasević

Geneva Internet Platform DigitalWatch

The Geneva Internet Platform is an initiative of:
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
République et Canton de Genève
DiPLO www.diplomacy.edu