Geneva Internet Platform
DigitalWatch
NEWSLETTER

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.

DIGITAL POLICY TRENDS IN NOVEMBER

1. New cybersecurity declarations and resolutions abound

November saw several new declarations and resolutions related to security in cyberspace, demonstrating once again the prominence of this topic on the international agenda.

At the opening of the global 13th Internet Governance Forum (12–14 November), French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, a high-level declaration on developing common principles for securing cyberspace. The declaration invites signatories to prevent damage to the public core of the Internet, and to contain the proliferation of malicious ICT tools and practices. *More on page 7*

In the UN framework, two resolutions on cybersecurity issues were adopted in the First Committee of the General Assembly (UN GA). The first resolution, proposed by Russia, reiterates (with some amendments) the norms and principles of responsible state behaviour in cyberspace outlined in the 2013 and 2015 reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security (UN GGE). It then calls for the establishment of an open-ended working group to further develop these norms and the ways for their implementation, on a consensus basis. The group should involve all interested states; hold consultations with business, NGOs and academia; and report to the UN GA in autumn 2020.

The second resolution, proposed by the USA, underlines the reports of the UN GGE and calls for the establishment of another GGE (with limited participation, based on 'equitable geographical distribution'), mandated to further study norms, rules and principles of responsible state behaviour, confidence-building and capacity-building measures, and how international law applies to the use of ICTs by states. The group is to report to the UN GA in autumn 2021.

While several UN member states expressed concerns over the fact that two 'separate, yet similar' resolutions were adopted, others noted that the two proposed processes are compatible. It remains to be seen how the resolutions are tackled in the full UN GA.

Trends continue on page 3

The Geneva Internet Platform wishes its readers a merry festive season!

Credit: Fancycrave on Unsplash

IN THIS ISSUE

Issue no. 36 of the *Digital Watch* newsletter, published on 7 December 2018, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila (Editor), Stefania Grottola, Đorđe Jančić, Marco Lotti, Grace Mutung'u, Nataša Perućica, Vladimir Radunović, 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/november2018

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.

Expert workshop on the 'Geneva Dialogue on Responsible Behaviour in Cyberspace'

The event took place on 1 and 2 November within the framework of the 'Geneva Dialogue on Responsible Behaviour in Cyberspace' project which analyses the roles and responsibilities of states, industry actors and civil society, and academic and tech communities in contributing to greater security and stability in cyberspace.

The discussion identified good practices and possible gaps in existing efforts and put forward recommendations for overcoming such gaps. The dialogue complements existing initiatives and aims to provide additional insights and recommendations on how different actors can contribute to greater stability and security in cyberspace.

The first in a series of webinar discussions on responsible behaviour in cyberspace was held before the workshop, with the remaining ones scheduled for the first half of December. A final report is expected to be published by the end of the year.

Cybermediation: The impact of digital technologies on the prevention and resolution of violent conflicts

The event took place on 7 November at the Palais des Nations within the context of the 2018 edition of Geneva Peace Week. It discussed how digital technologies impact mediators in their activities, exploring the opportunities these technologies offer and the risks they pose.

The event is part of the Cybermediation initiative, launched earlier in 2018, to respond to the fact that conflicts increasingly have cyber dimensions and to the need for those who work to prevent conflicts to catch up with this trend. In particular, the discussion tackled the application of AI, social media platforms, and the engagement of the private sector in peace mediation.

UN Forum on Business and Human Rights

The 7th edition of the UN Forum on Business and Human Rights took place on 26–28 November, and featured discussions on topics related to the *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*.

The Forum addressed different technology-related issues, with specific events on disruptive technology, on the role of tech companies in the protection of human rights, and on the application of blockchain to scale up the principle of due diligence. The two discussions on disruptive technology covered issues related to the protection of human rights in the context of the ongoing developments in automation and AI.

Other events addressed the responsibilities of the private sector in ensuring the protection of human rights and advocating for stronger public policy deliberations within governments. Finally, the use of blockchain was explored as an application to scale up human rights due diligence in the case scenarios of supply chains.

Public International Law Day 2018

The event, on 27 November, was organised by the Directorate of International Law of the Federal Department of Foreign Affairs, in co-operation with the Geneva Internet Platform. It focused on the application of international law in cyberspace.

Digital transformation and cybersecurity featured as main topics of discussion. To achieve an inclusive, free, and stable digital environment as a paradigm of peace and security and respect for human rights, innovative approaches are needed to face these digital developments. The event addressed the current challenges posed by digital transformation and cybersecurity threats, with a multi-disciplinary approach involving perspectives from the foreign policy and diplomatic field, the technology field, and the legal field.

DIGITAL POLICY TRENDS IN NOVEMBER

Continued from page 1

Also in the field of responsible behaviour in cyberspace, the Global Commission on the Stability of Cyberspace proposed six new norms. These proposals encourage state and/or non-state actors to avoid tampering with products and services, refrain from commandeering ICT devices into botnets, create transparent frameworks to assess when and whether to disclose vulnerabilities, promote cyber hygiene, reduce and mitigate significant vulnerabilities, and refrain from offensive cyber operations.

Within the EU, the European Commission adopted an updated version of the EU cyber defence policy framework, which identifies six priority areas for cyber defence: development of cyber defence capabilities, protection of the EU Common Security and Defence Policy, communication and information networks, training and exercises, research and technology, and civil-military and international co-operation.

In Asia, member states of the Association of Southeast Asian Nations (ASEAN) issued two joint statements on cybersecurity-related co-operation: one with Russia, and one with the USA. Both declarations touch on the need to promote and elaborate on already proposed norms of responsible behaviour of states in cyberspace and to tackle the use of ICTs for terrorist purposes.

With so many new declarations, the real test will be in their implementation.

2. Calls for ethical considerations in development of artificial intelligence systems

Fast developments in artificial intelligence (AI) have pushed discussions to the mainstream. Not only are policymakers and technologists discussing the issues surrounding AI, but so are citizens. The discussions have now entered a new domain, with a focus on ethical considerations.

'There can be no AI [...] if reflection with an ethical dimension is not conducted', the French President noted during the IGF. Macron spoke about his intention to 'spearhead' the creation an intergovernmental initiative on AI, similar to the Intergovernmental Panel on Climate Change. The panel should co-operate with civil society, scientists, and innovators, and reflect on the ethical, tehnical, and scientific dimensions of AI.

Many IGF sessions reflected on the need to consider ethical principles in the design and use of AI. For AI applications to be 'pro-people', ethical aspects have to be carefully considered. However, several open questions remain: Which ethical concepts are we actually looking at, considering that there is no universal agreement on what is ethical? Can we really embed ethics into code? And who should bear the main responsibility?

Another thread of discussions focused on the relation between ethics and law. While some ethical rules are codified into law, they should not be seen as a substitute for legislation. When we look at how to ensure AI is pro-people, we should take into account both ethical principles and legal frameworks.

This issue was also raised by the UN Rapporteur on extreme poverty and human rights, Prof. Philip Alston. In a recent statement, he drew attention to the limitations of ethical frameworks, rooted in the fact that there are no generally agreed definitions of ethical concepts. Human rights, however, are embedded in law. This is why the use of AI 'needs to be bound by the rule of law and not just an ethical code'.

The underlying message of all these discussions is that we should look more carefully into how to practically ensure that AI applications are consistent with both law and ethics.

3. The gig economy in focus again

There is a growing realisation that existing rules are not reflecting the realities of the changing labour market. A report released by the Organisation for Economic Co-operation and Development (OECD) on *The Future of Social Protection*, shows that work patterns are increasingly deviating from the traditional model of a full-time dependent employee towards self-employment or the 'gig worker' pattern. Because traditional social protection systems were designed for the former model, they may not be adequate to protect workers in the 'gig economy'.

Governments are increasingly becoming aware of the need to adapt their regulations to the changing work environment. The UK, for example, is expected to publish new rules on the future of work, to include, among others, an extension of employment rights to self-employed gig economy workers. The UK's approach towards regulating work in the gig economy is expected to have a significant impact on other economies, especially in Europe.

One of the issues that continues to generate controversy is the status of gig workers: Are they employees or independent contractors? In a recent case from Australia, the food delivery company Foodora was taken to court over classifying a rider as an independent contractor. The Australian Fair Work Commission ruled that the rider was working for Foodora and his work was not an independent operation. The company has finally admitted that their riders were more likely to be employees than independent contractors.

This judgment can impact the workforce classification in other gig economies around the world, including in relation to Uber Eats and Deliveroo (food delivery services), but also other sectors of the gig economy.

Credit: Mark Warner

DIGITAL POLICY: DEVELOPMENTS IN NOVEMBER

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.*

Global IG architecture

increasing relevance

During Paris Peace Week, French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, a high-level declaration on developing common principles for securing cyberspace. *More on page 7.*

Facebook and Google have signed Tim Berners-Lee's Contract for the Web, which appeals to governments, companies, and netizens to improve Internet accessibility, privacy, and confidentiality of user data, and to keep the Internet free and safe.

Sustainable development

same relevance

During the International Telecommunication Union (ITU) Plenipotentiary Conference (ITU-PP18), member states approved a revised resolution on the use of ICTs to bridge the digital divide. The ITU is to continue its task of preparing indicators for measuring the digital divide, collecting statistical data, and measuring the impact of ICTs.

The OECD's latest report on *Bridging the Digital Gender Divide: Include, Upskill, Innovate* reconfirms that women have less access to technology, services, and educational opportunities in information technology than men.

Security

increasing relevance

Two new resolutions on cybersecurity issues – one proposed by Russia and one by the USA, – have been adopted by the First Committee of the UN GA. *More on pages 1-3.*

The Global Commission on the Stability of Cyberspace (GCSC) has proposed six new norms for state and non-state behaviour in cyberspace. According to its Commissioners, the GCSC may still work on the development of a few additional norms, but will now put more focus on exploring ways to steer other processes with its proposed norms.

The EU has updated its cyber defence policy framework, which now identifies six priority areas, such as the the development of cyber defence capabilities, promoting civil-military co-operation and international co-operation, and developing research and technology capacities.

E-commerce & Internet economy

same relevance

The workforce landscape is changing with the gig economy, and traditional social protection systems may no longer be adequate, according to a new OECD study. New rules for the gig economy are expected in the UK, while in Australia, the Fair Work Commission ruled that a driver for a food delivery company was an employee, and not an independent contractor.

Economic ministers at the 33rd ASEAN Summit agreed on new e-commerce rules that aim to facilitate cross-border transactions and promote confidence in the use of e-commerce.

The fourth largest cryptocurrency, Bitcoin Cash, which emerged from a Bitcoin fork in August 2017, has split further, following a dispute over its consensus mechanisms. Visa will be deploying a blockchain-based digital identity system for cross-border payments.

Digital rights

increasing relevance

The UN GA's Third Committee adopted a resolution on the right to privacy in the digital age, which calls on states to prevent privacy violations, and on businesses to inform users 'in an intelligible and easily accessible' manner about the collection, use, sharing, and retention of their data (including biometrics) that may affect their right to privacy.

Freedom House's report *Freedom on the Net 2018: The Rise Of Digital Authoritarianism* shows that Internet freedom has declined for the eighth consecutive year.

Facebook announced it will appeal the UK's Information Commissioner's Office's fine over the Cambridge Analytica scandal.

Google's takeover of UK-based AI lab Deepmind has raised concerns over the company's future access to patients' health data collected from UK's National Health Service (NHS).

Jurisdiction & legal issues

increasing relevance

Parliamentarians from countries forming part of the International Grand Committee on Disinformation and Fake News have signed a declaration on the Principles of the Law Governing the Internet.

France has reached an agreement with Facebook to allow government officials to monitor the company's hate speech policies and removal procedures.

An Indian High Court ruled that an e-commerce platform is liable for counterfeit goods sold on its platform, even though the items are sold by third parties.

Infrastructure

increasing relevance

Elon Musk's SpaceX has received approval by the USA's Federal Communications Commission (FCC) to send over 7000 very low Earth-orbit satellites to provide global Internet connectivity from space.

A resolution on self-driving cars by the UN Economic Commission for Europe (UNECE) makes several recommendations for automated driving systems and their users.

Net neutrality

decreasing relevance

AT&T CEO is urging the US Congress to pass net neutrality laws in order to avoid a patchwork of state legislation.

US senators have asked major wireless carriers for a written statement regarding throttling of video services.

New technologies (IoT, AI, etc.)

increasing relevance

Countries announce new AI plans. Malta has established a task force to develop a national strategy on AI. The aim is 'to position Malta among the top 10 countries in the world with an AI policy'. Germany will invest €3 billion in research and development by 2025. The UAE has established a lab to develop regulations that will govern the use and applications of AI, 3D printing, and other emerging technologies.

The Committee of Ministers of the Council of Europe calls on member states to evaluate the impact of algorithmic systems on human rights and fundamental freedoms. A second document warns about the 'manipulative capabilities' of algorithmic processes, and the risks of using large amounts of personal data for such process.

The UN Special Rapporteur on extreme poverty and human rights has called for more transparency around AI.

AHEAD IN DECEMBER

For more information on upcoming events, visit https://dig.watch/events

DIGITAL IDENTITIES: ISSUES AND CASES

Low and middle income countries are rolling out sophisticated digital identification systems. Will they be a panacea for social and economic inclusion, or are they another way to control people's personal information?

For generations, people in the global south acquired identity culturally. In some places, children get their first identity during their naming ceremony while others acquire their permanent names after initiation rites. In modern states, individuals take state identification in order to access government services such as passports, social welfare, and higher education. State-backed identification is integral to accessing services provided by non-state actors.

For example, those without identification documents cannot access banking services. New digital means of identification, such as mobile phone numbers, are expanding traditional notions of financial inclusion. Under the World Bank's Identity for Development (ID4D) low and middle income countries are rolling out nationwide digital identification systems.

Demand for identification services is on the rise. This is partly driven by the aspiration to account for every person on Earth under the sustainable development goals (SDGs) as reflected in the theme 'leave no one behind'. But a gap has been identified in delivering the SDGs: Over half of the world's population, found in the global south, is not identified.

What are digital identities for?

Identification can assist states better plan for their needs. With the interconnectedness provided by digital technologies, states can analyse identified individuals, anticipate their needs, and apply available resources to meet those needs most efficiently. Coupled with developments such as mobile telephony and digital footprint tracking, states can also build comprehensive profiles on the social, political, and economic behaviours of their people. Such information can be applied in planning for future generations, designing disaster and emergency response, and building new economic activities. The same information could also be used for political manipulation, stifling of expression, exclusion of dissenters, and other similar motives.

The issues around digital identities

Digital ID can take different forms, with governments choosing the extent to which to consolidate data about each person. Kenya is integrating its numerous state and private identification databases to improve efficiency in delivering services that depend on identification. India is creating the world's largest identification registry, Aadhar, that targets identifying previously unidentified populations. In China, state-issued smart cards record and analyse a person's entire relationship with the government by tracking every transaction an individual has with the state. This is used to build the person's social credit. This model is also referred to as 'a single source of truth'.

If not designed carefully, digital ID programmes can create databases that may easily abrogate a citizen's rights to privacy. They are designed to centralise data collection and analysis, increasing the risk of misuse of the data, for example in unwarranted surveillance. Where data collection is flawed, sections of citizens (most often the marginalised groups) are excluded from the databases and consequential services. The problem is compounded when a country does not have a data protection framework.

Aadhar has been challenged regarding data sharing. Even with a supreme court order prohibiting the linking of Aadhar data with the voters register, investigators recently found that India's electoral commission still accessed and related the two registers.

The need for safeguards

Human rights advocates describe these digital ID programmes as latent tools for state surveillance. Without safeguards, states can abuse the vast knowledge acquired from the collection of citizens data through information controls. Vulnerable populations such as refugees and those in need of social services from authorities may also be misrepresented in the digital registries, in effect deepening existing inequalities. How then can we ensure that digital identity protects individuals and groups from harm?

One solution is through shifting the power in digital identification from the authorities to the person. This can be achieved in part through people-centric data protection frameworks that guarantee protection of the right to privacy, promote responsible data sharing, and ensure information security. Research on autonomy promoting digital identity is underway.

When it comes to the problems associated with platforms storing large amounts of identification information, one of the explored solutions relates to a self-sovereign identity (SSI) approach. Under SSI, individuals store their own digital identification in virtual wallets and produce this identification at their own discretion as they navigate online spaces. SSI is a departure from a centralised storage of data. Once a user acquires SSI, they are solely responsible for choosing where to use their digital identification. SSI is based on principles of control, access, transparency, persistence, portability, interoperability, consent, minimisation, and user protection.

Wherever applied, digital ID converges with the organisation of society. As proponents of the SDGs support the adoption of these systems, they ought to also promote digital ID models that facilitate the flourishing of society and are in line with human rights.

UNDER THE BONNET OF THE 'PARIS CALL'

When he presented the Paris Call for Trust and Security in Cyberspace at the IGF in Paris last month, President Macron said that cyberspace has become a place of conflict, and the response to this challenge should not be limited to defence, but should also incorporate 'law and co-operation'. So what is the Paris Call inviting stakeholders to do?

Building on previous documents

Presented as a high-level declaration on developing common principles for securing cyberspace, the call invites stakeholders – states, international organisations, the private sector, NGOs – to work together and 'uphold international law in cyberspace, protect rights online, fight against destabilising activities and ensure the security of digital products'.

The Paris Call takes inspiration from previous documents adopted in the context of other Internet governance and digital policy processes.

The document builds on language from the Tunis Agenda for the Information Society, outlining that it is the responsibility of states and other stakeholders 'in their respective roles', to enhance trust, security, and stability in cyberspace.

Without mentioning it specifically, it resonates with the UN GGE report of 2013, in reaffirming that international law is applicable to cyberspace. And it emphasises the importance of norms during peacetime and of confidence-building measures, thereby implicitly acknowledging the results of the UN GGE of 2015.

Lastly, the Paris Call has also partially integrated several of the norms proposed by the Global Commission on the Stability of Cyberspace.

Commitments to trust and security in cyberspace

The Paris Call condemns 'significant, indiscriminate, or systemic harm' of cyber-attacks to individuals and critical infrastructure in peacetime, and invites support for victims during both peacetime and armed conflict. Reflecting on the need to strengthen protection against cybercrime, the declaration places the Budapest Convention on Cybercrime as the key tool. It further calls for increased security of products, and recognises the responsibility of key private sector actors in this regard.

The Call also outlines the importance of multistakeholder co-operation in the development of new cybersecurity standards, and encourages 'responsible and coordinated' disclosure of vulnerabilities. Supporting broad digital co-operation and enhanced capacity-building efforts, the Call relates implicitly to the UN High-Level Panel on Digital Cooperation, and underlines the need for a strengthened multistakeholder approach towards cybersecurity and trust.

Signatories of the Call commit to working together and implementing 'cooperative measures' to, among other, prevent

- harm to individuals and critical infrastructure.
- damage to the general availability or integrity of the public core of the Internet.
- foreign intervention in electoral processes through malicious cyber activities.
- ICT-enabled theft of intellectual property for competitive advantage.
- the proliferation of malicious ICT tools and practices.
- non-state actors from 'hacking-back' ('conducting offensive cyber operations' was the term used in previous versions of the Call, yet replaced, likely because this term is used primarily in relation to state conduct).

Other commitments relate to strengthening the security of digital products and services, and promoting advanced cyber-hygiene for all.

Finally, the declaration calls for the widespread acceptance and implementation of international norms of responsible behaviour. It is interesting that the term 'development of norms' has been removed in the final draft, possibly signalling diminished support for developing further norms.

What's next?

Hundreds of governments and other entities – including most European countries, the lead Internet industry, the Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Society – have signed the Paris Call. But beyond the signatories, it is also notable that, out of the five permanent members of the UN Security Council, China, Russia and the USA are yet absent.

As outlined at the end of the Call, the signatories will reconvene and assess the progress during the Paris Peace Forum (PPF) in 2019, as well as during the IGF 2019 in Berlin. This is signalling that the PPF will continue, but also that signatories of the Paris Call do not intend to duplicate efforts, but rather to feed in/be in sync with the IGF process, something appreciated by a number of signatories.

It is also worthwhile mentioning that Macron even suggested, in his IGF speech, that the IGF be entrusted with monitoring the evolution of the Paris Call's text, recording the supporters, and identifying the co-operation initiatives and measures necessary to reach its goals. Whether the IGF actually takes up this role is to be seen.

CROSSWORD

THE IGF IN A NUTSHELL

In November, much of the Internet governance and digital policy community had its eyes on the 13th IGF meeting. The three-day event featured around 130 sessions in which participants from governments, intergovernmental organisations, technical bodies, and private companies alongside end-users discussed multiple Internet-related issues. Privacy and data protection, digital divide, cybersecurity, blockchain, and AI were only some of the topics tackled.

Are you up-to-date with the IGF and this year's discussions? Try this crossword and find out. And if you want to learn more, visit the IGF 2018 dedicated space in the Digital Watch observatory where you will find reports from almost all sessions, daily summaries of the discussions, and a final report rounding up the issues that mattered most.

IGF Report

Published on Tuesday, 27th November, 2018

FINAL REPORT FROM THE 13th INTERNET GOVERNANCE FORUM

dig.watch/igf2018

IGF: CHANGE NEEDED TO STAY RELEVANT

The IGF will need to adapt quickly in order to remain relevant in the fast changing digital world. This was the writing on the 'IGF wall' in keynote addresses, workshops, and corridor discussions.

For the first time in the IGF's history, the annual meeting was presided over by both the host country's head of state and the UN Secretary-General. In sharp contrast with this officialdom, government representation was low compared to civil society and the business community. The Secretary-General encouraged the IGF to reach out to governments, in particular those from developing countries.

One of the potential reasons for dwindling government participation is that the IGF 'needs to produce more than just debate and reflection'. Last year, the IGF made a step forward by gathering conclusions of discussions in the form of Geneva Messages. This year, French President Emmanuel Macron made the following proposals for the IGF reform:

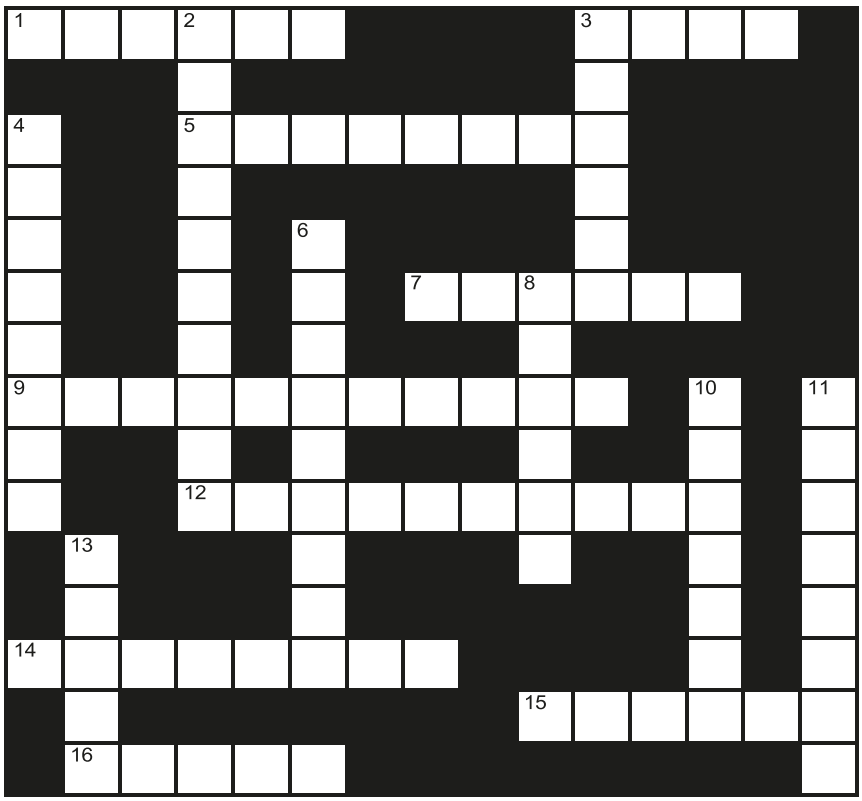
- The IGF needs to reform, according to Macron, 'to become a body producing tangible proposals'. Switzerland, France, and Germany, as the previous, current, and next host, have also been supporting more concrete outputs in the IGF deliberations.

Continued on page 2

IN THIS Report

Commentary 1–3
Social Media monitor 2
Data Analysis: What the transcripts say 4
Summarising IGF 2018 5–11
Towards IGF 2019 12
Contributors 12

The IGF 2018 Report is prepared by the Geneva Internet Platform with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation



Across

1 The first IGF meeting was held 12 years ago in _____. (6)

3 Many argued that, with the growing reach and scope of online platforms, the ____-regulatory model is no longer enough to ensure that these platforms act in line with the interests of end-users. (4)

5 The IGF intersessional work includes dynamic coalitions and best _____ forums on issues such as community connectivity, blockchain, cybersecurity, and AI. (8)

7 Child safety online remained a prominent issue at the IGF, and it was noted that measures to protect children in the digital space should be put into the context of children's ____. (6)

9 Although there was a lot of debate in Paris about the future of technology, one important topic was missing from the discussions: the rights of future _____. (11)

12 This year, the IGF was organised for the _____ year. (10)

14 This year's IGF meeting was opened by the UN Secretary General, Mr Antonio _____. (8)

15 The next IGF (2019) will be held in _____, Germany. (6)

16 The IGF draws its mandate from the _____ Agenda for the Information Society, adopted in 2015 in the context of the World Summit on the Information Society. (5)

Down

2 The interplay between emerging technologies and _____ was also widely discussed, with a focus on the need to ensure that the young generation is prepared for tomorrow's job market. (10)

3 The discussions around misinformation and fake news emphasised the need for democracies to navigate the tension between free ____ and addressing fake news. (6)

4 Introduced in 2017 as an innovation within the IGF process, the IGF Key _____ outline the main takeaways of the discussions around thematic areas. (8)

6 When it comes to cybersecurity, IGF stakeholders reiterated the need to define rules of _____ in cyberspace. (9)

8 The discussions on human rights were dominated by issues related to threats to freedom of expression and privacy, and the persistent _____ digital divide. (6)

10 The most prominent issue throughout IGF 2018 discussions was AI, and many discussions focused on the need to integrate _____ considerations in the design and use of AI systems. (7)

11 One of the underlying messages of IGF 2018 was that the Forum needs to adapt quickly in order to remain _____ in the fast-changing digital world. (8)

13 'The Internet of _____' was the overarching theme of the Paris IGF. (5)

Across: 1 Athens, 3 Self, 5 Practice, 7 Rights, 9 Generations, 12 Thirteenth, 14 Guterres, 15 Berlin, 16 Tunis.
Down: 2 Employment, 3 Speech, 4 Messages, 6 Behaviour, 8 Gender, 10 Ethical, 11 Relevant, 13 Trust.