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 OCTOBER

The trends in October revolve around the tech giants; their data-based business models; and the backlash they are facing over their practices, their large revenues, and their even larger dominance. Is the position of tech giants starting to weaken?

1. Data breaches continue; tech giants face tougher backlash

When everyone thought the Cambridge Analytica scandal was water under the bridge, out came the revelations of two new major breaches.

A software glitch on Google+ allowed outside developers to potentially gain access to the private data of over 500,000 users, between 2015 and March 2018. Although the platform is now shutting down for consumers, Google failed to disclose the bug. According to the *Wall Street Journal*, an internal memo prepared by the company's legal and policy staff warned that disclosing the incident would trigger an 'immediate regulatory interest' and cause reputational damage.

In a second case, Facebook revealed that a security issue had affected 30 million user accounts. Hackers exploited the 'view as' feature to get access to log-in details and private data such as usernames, phone numbers, e-mail addresses, gender, and religion.

With so much market dominance (based primarily on the data business model) and access to private data, governments and users have grown increasingly uneasy and impatient with the tech companies' inability to keep private data secure. The continual breaches are also raising tougher questions on accountability and consumer protection.

Amid these debates, the toughest criticism this month came from Brussels. Data protection officers (DPOs) gathering for the annual International Conference of Data Protection and Privacy Commissioners sent a clear message: Companies need to bring their data-related practices in line with higher standards of protection for the rights of users.

Trends continue on page 3

Apple CEO Tim Cook did not mince his words, during the 40th International Conference of Data Protection and Privacy Commissioners: 'The desire to put profits over privacy is nothing new... We shouldn't sugarcoat the consequences. This is surveillance. And these stockpiles of personal data serve only to enrich the companies that collect them.' *More digital policy updates on pages. Credit: ICDPPC*

IN THIS ISSUE

Issue no. 35 of the *Digital Watch* newsletter, published on 6 November 2018, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Cedric Amon, Stephanie Borg Psaila (Editor), Dylan Farrell, Andrijana Gavrilović, Stefania Grottola, Arvin Kamberi, Clement Perardnaud, Natasa Perućica, Vladimir Radunović | 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/october2018

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.

World Trade Organization (WTO) Public Forum 2018t

The 2018 edition of the WTO Public Forum, on 2–4 October, focused on Trade 2030, and addressed the impact of technologies on the trading system, while providing a glance into the future. The topics of discussion – economic growth, creation of jobs, and sustainable development – tried to answer the cross-cutting question across many sessions: Is today's global trading system equipped to face the changing environment in which we live?


SUMMARY REPORT WTO PUBLIC FORUM 2018

Geneva Internet Platform DigitalWatch

Report prepared by the Geneva Internet Platform with support from DiploFoundation

'Trade 2030' was the main topic at this year's World Trade Organization (WTO) Public Forum (2–4 October). The event provided a glimpse into the future and focused on the impact of technology on the trading system. Participants gathered at the headquarters of the WTO, in Geneva, to discuss how trade can further contribute to economic growth, the creation of jobs, and sustainable development. The cross-cutting question that many of the sessions addressed was: Is today's global trading system equipped to face the changing environment we live in?

OVERVIEW

The inequality between those benefiting from technology-enabled trade and those lagging behind was the backdrop for discussions on how to narrow the divide, and utilise trade instruments in achieving the sustainable development goals (SDGs). Discussions also focused on data flows, the need to create more jobs to counter automation-related issues, and the evolution of artificial intelligence (AI), online platforms, and big data analytics on services for trade. The forum addressed the harmonisation of regulatory frameworks with regard to cybersecurity, privacy, and data governance, while stressing that investment, regulation, and industrial policy will need to be smartly combined to promote development and face the challenges to come.

The GIP reported on digital policy-related sessions from the WTO Public Forum. Read our session reports, and download our final report from the forum.

#Cybermediation: What role for blockchain technology and natural language processing AI?

The event, delivered in situ and online on 5 October, hosted by the GIP as part of the #Cybermediation Initiative, focused on the role of blockchain and AI in supporting mediation activities. Technology will not replace human intelligence and ingenuity, but will provide pragmatic approaches.

Speaking on AI, Dr Katharina Höne argued that as a 'study of systems that can make intelligent decisions', AI can complement diplomacy and mediation by saving resources and time, generating new insights, supporting the work of practitioners, and, ultimately, contributing to better conflict resolution. When it comes to blockchain, Mr Dejan Dincic explained that despite the technology being around for a number of years, there are yet no large-scale applications. Using a hypothetical scenario in which blockchain could be used to monitor and implement agreements, Dincic explained that blockchain could play an important role because of its objective, neutral, transparent, and decentralised nature.

Read a more in-depth summary of the discussions and view our recording of the event.

The EU General Data Protection Regulation (GDPR) and international data flows

The event, on 10 October, hosted by the European Union Delegation to the UN in Geneva and the Permanent Mission of Austria in Geneva, in co-operation with the GIP, discussed the EU's GDPR which entered into effect on 25 May 2018. Panellists described it as an important achievement for the protection of EU citizens' personal data, and in the search for balance between data protection and the legitimate interests of business operators. They discussed the increasing convergence of data protection norms at international level, and the impact on international data flows from the perspectives of both citizens and businesses.

UNCTAD World Investment Forum 2018

Internet-based technologies have changed the way goods and services are produced and consumed. The digital economy has also created a shift in global investments.

The annual forum organised by the United Nations Conference on Trade and Development (UNCTAD), on 22–26 October, addressed the challenges in mobilising investment towards the development of the digital economy, and the innovative practices and policies that help facilitate such investment. During the discussions, investment guides (or i-guides, which provide up-to-date information for investors), were lauded as a helpful tool.

Some sessions also underlined the role of blockchain as a means of development-oriented investment which can help improve access to finance, supply chain management, digital identities, and public registries, especially for industries linked heavily to the SDGs, such as agriculture, healthcare, and transportation. *Read our reports from digital policy-related sessions during the forum.*

This icon indicates that there is more background material in the digital version. Alternatively, visit **https://dig.watch** for more in-depth information.

DIGITAL POLICY TRENDS IN OCTOBER

Continued from page 1

It is the recognition that data governance and digital business models are central to the debate on the future of the digital economy that has brought on this tough stance from the DPOs, who are also realising that their role is vital. This realisation is already weakening tech giants and creating divides. In Brussels, Apple's CEO Tim Cook called for tougher rules in the USA, similar to the EU's GDPR.

The future of the data economy will depend on finding the right balance between tackling privacy, data protection, consumer protection, and security issues on the one hand, and sustaining data flows which are fuelling many economies on the other.

2. Digital tax: Go-it-alone approach a game-changer

The EU's planned tax, which will impose a 3% levy on tech companies' revenues, could quite possibly be rolled out by the end of the year, EU's Economic and Financial Affairs Commissioner Pierre Moscovici announced to the BBC. The tax is aimed specifically at tech giants: those with a total annual revenue of €750 million or above, and yearly EU taxable revenue of €50 million+.

Yet, rifts are still wide. Some are frustrated by the lack of progress; others are opposed to the plans.

Frustrated by the slow developments at the EU and on the global level (mainly the work of the Organisation for Economic Co-operation and Development (OECD) which has been on a global tax framework), the UK chancellor Philip Hammond said that the UK would 'go at it alone', and announced a new UK digital services tax in its budget. The tax will come into effect in 2020, and will only be applied 'until an appropriate long-term solution is in place'.

A small group of EU countries, including Ireland, the Czech Republic, Finland, and Sweden, are still unconvinced about the EU's plans for a digital tax. One of their main reasons is that countries should give the OECD more time to develop a global tax framework for companies operating digitally.

The USA has also criticised the EU's plans, calling the planned tax a discriminatory one.

A potential solution, suggested by France and supported by Austria, is to introduce a sunset clause in the EU's tax plans. The tax would end once an agreement is reached at global level. This is similar to the provision introduced by the UK.

While developments are therefore speeding up in the EU (further delays can complicate matters due to Brexit and European elections next year), the new go-it-alone approach changes the dynamics of the game. Governments are ready to act unilaterally, and to quickly transform the tech backlash into monetary action.

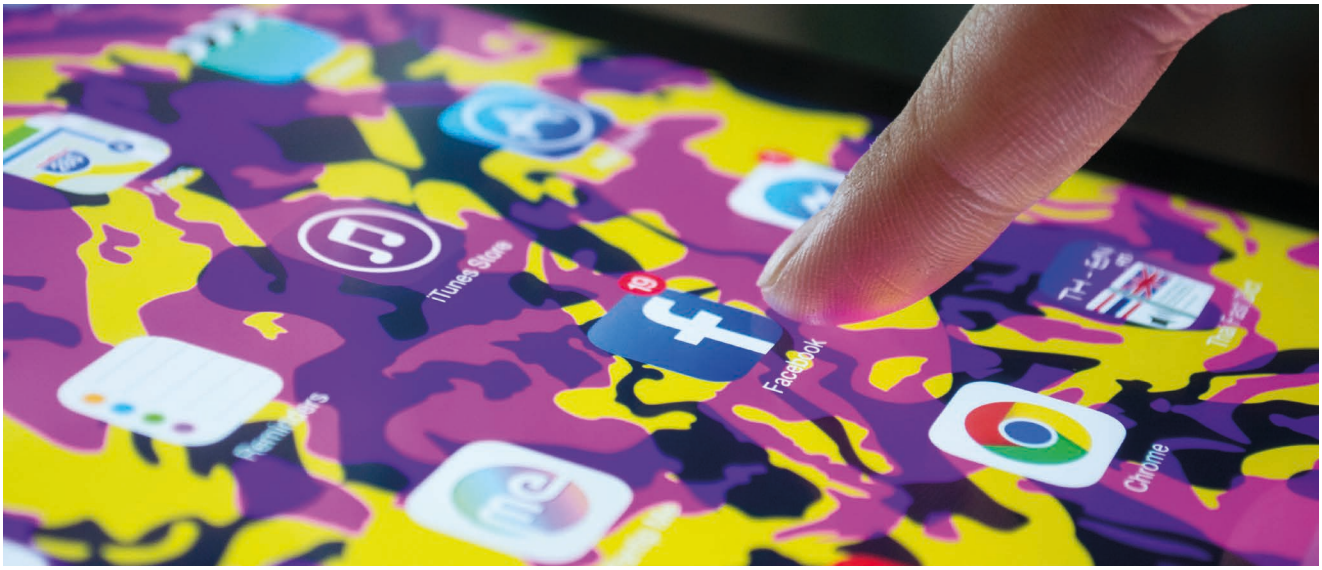
3. Antitrust rules: A change in direction?

Undoubtedly, major tech companies have developed enormous economic and market powers. Their monopolistic status has been raising concern among the general public and governments.

Although antitrust and anti-monopoly rules are theoretically meant to address these situations, their application has been limited. Evolving quickly in the USA is the debate that such rules should be adapted to protect competition *per se*, rather than applied only in cases where there is a monetary loss for consumers.

One of the potential solutions for addressing the dominant market power of tech giants is to adapt the application of these rules, according to Tim Wu, the professor at Columbia Law School who is also credited with coining the term 'net neutrality' (read a review of Wu's book). Other solutions include breaking up the biggest monopolies, renewing the practice of reviewing mergers, and renewing the practice of bringing major antitrust actions against the biggest companies.

In the EU, tech giants have already been slapped with several antitrust cases. Given the role of data in tech companies' business models, the next battle will inevitably revolve around their use of data in many of their business practices.



DIGITAL POLICY: DEVELOPMENTS IN OCTOBER

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

same relevance

During the fifth EU–US Cyber Dialogue, the EU and USA endorsed the previous work of the UN Group of Governmental Experts (UN GGE), in particular the consensus reports of 2013 and 2015. They also expressed willingness to participate in a new UN GGE to discuss the applicability of existing international law to cyberspace. *More on page 7.*

Sustainable development

same relevance

In its latest report, *Trade and Development Report 2018: Power, Platforms and the Free Trade Delusion*, UNCTAD addressed the state of the world's economic system and emphasised the need for more policies that favour inclusion in the global digital economy.

Policies needed to achieve affordable Internet are developing too slowly, according to the *2018 Affordability Report* published by the Alliance for Affordable Internet (A4AI). Over 60% of the countries studied still have prohibitive connection costs; island nations experience the highest costs to connect.

Security

increasing relevance

Two cybersecurity-related resolutions have been introduced in the First Committee of the UN General Assembly. *More on page 7.*

Facebook revealed that hackers stole access tokens of about 30 million users. The breach took place in September. The hackers exploited a vulnerability in the code of the feature known as 'View As', which gave them access to the profiles and log-in details.

Google also revealed that a software glitch on Google+ gave outside developers potential access to users' private data between 2015 and March 2018. The company patched the bug in March 2018, but did not disclose it for reputational reasons. The company also announced it is shutting down Google+ for consumers.

In a statement submitted to Australia's parliament on the proposed Access and Assistance Bill 2018, Apple called for stronger encryption, and expressed concern that the bill favours the government's interpretation of the legal terms and technical facts.

E-commerce & Internet economy

increasing relevance

Canada, Mexico, and the USA reached a deal to replace the North American Free Trade Agreement (NAFTA). The new US-Mexico-Canada Agreement (USMCA) includes chapters on digital trade and data, and controversial provisions such as a ban on restrictions of data transfers across borders.

Debates on taxing the Internet economy picked up, as the EU said it will roll out an EU-wide tax 'within 60 days', while Britain went ahead with unveiling a new tax for tech giants. *More on page 3.*

The competitiveness landscape is being radically altered by the impact of the fourth industrial revolution and digital technology, the World Economic Forum's *Global Competitiveness Report 2018* concluded. Global economic health can be positively impacted by a return to greater openness and integration; yet, there is a need for new policies to improve conditions of those adversely affected by globalisation.

Digital rights

increasing relevance

Apple CEO Tim Cook praised the EU's data protection rules and called for a similar development in the USA. Speaking during the annual data protection commissioners' meeting in Brussels, he also warned against the threat of 'data industrial complex'.

Facebook was fined €565,000 (the maximum fine allowed) by the UK Information Commissioner's Office (ICO) for its involvement in the Cambridge Analytica scandal. The ICO said that Facebook allowed third party applications to access users' data without their consent.

The social media network also removed 559 pages and 251 accounts of several alternative media pages, arguing that the accounts had engaged in 'inauthentic behaviour'.

Jurisdiction & legal issues

increasing relevance

The EU-US Privacy Shield underwent its second legal review, amid concerns over its unsound legal foundation, and the lack of compliance by US companies. The Commission will report on the review's conclusions by the end of the year.

Representatives of online platforms, social networks, and the advertising industry presented roadmaps to implement the EU Commission's Code of Practice on Online Disinformation. The roadmaps plan concrete action and best practices to tackle disinformation and the spread of fake news.

Infrastructure

same relevance

ICANN rolled out the new cryptographic key that protects the Domain Name System (DNS). The change is essential to the Domain Name System Security Extensions (DNSSEC) protocol which secures the Internet's foundational servers.

US President Trump signed a presidential memorandum instructing the Commerce Department to develop a national 5G spectrum strategy. The strategy is expected by July 2019.

Net neutrality

same relevance

The US Department of Justice (DOJ) sued California and blocked its new net neutrality law from entering into force. The DOJ argued that the new legislation, which bans numerous free-data plans that exempt consumers from data limits when streaming videos and music, is illegal and harms consumers.

New technologies (IoT, AI, etc.)

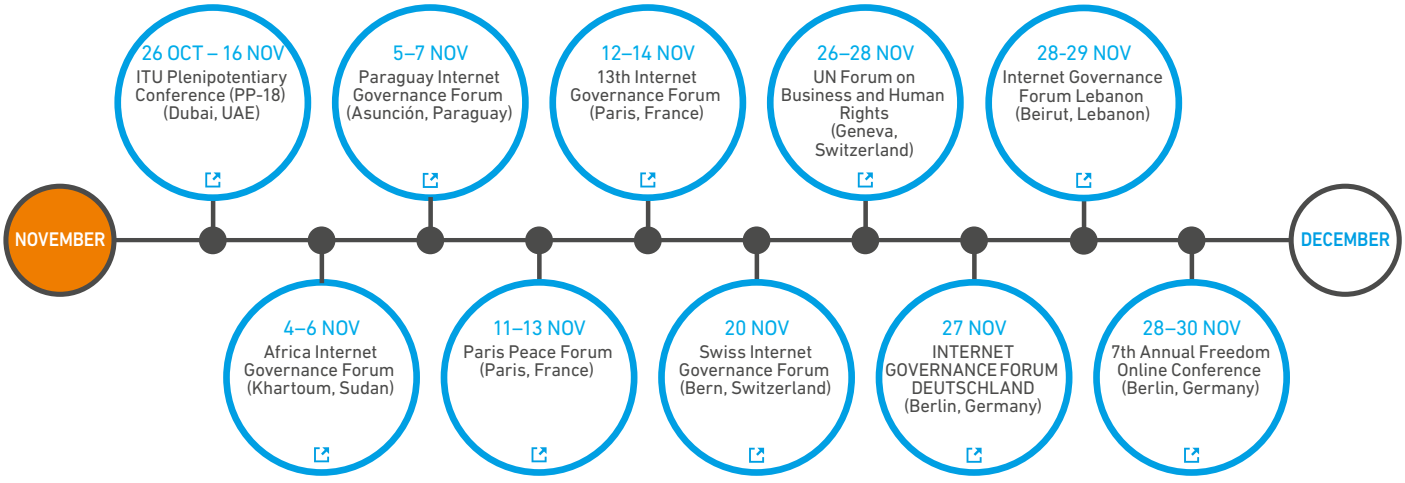
increasing relevance

Data protection authorities from over 15 countries adopted a Declaration on Ethics and Data Protection in Artificial Intelligence during their annual meeting in Brussels. It lists principles that should guide the design, development, and use of AI, including fairness; continued attention, vigilance, and accountability for the potential effects of AI systems; transparency and intelligibility; responsibility and the application of privacy by default and privacy by design approaches; empowerment of individuals; and reducing and mitigating biases and discriminations.

The UK's new Code of Practice for Consumer IoT Security provides guidelines on how businesses and organisations involved in developing, manufacturing, and retailing products can achieve a 'secure by design' approach.

Discussions on the use of blockchain for voting picked up ahead of the US mid-term elections in the USA.

AHEAD IN NOVEMBER



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

BLOCKCHAIN'S (IN)COMPATIBILITY WITH THE GDPR: UNPACKING THE DEBATE

The rapid development of blockchain in many sectors of the digital economy has been interpreted as both an immense opportunity and an imminent threat to the enforcement of the rights to privacy and data protection. Its compatibility with legal frameworks remains an open question, and will be crucial deciding its fate.

With the GDPR entering into force on 25 May 2018, the EU significantly reshaped its data protection regime, and imposed new obligations and responsibilities for individuals and organisations with regard to the processing of personal data of EU citizens.

Inevitably, blockchain's compliance with the GDPR emerged as a key issue for policymakers and companies, as the decentralised nature and operating principles of this technology raise significant challenges.

And so, what are the main tensions between blockchain and the GDPR? As detailed in the EU Blockchain Forum's recent report on Blockchain and GDPR, the main tensions revolve around the identification and obligations of data controllers and processors, the anonymisation of personal data, and the exercise of certain data subject rights (such as the right to erasure).

Issue #1: Identifying the data controller and processor

Data protection regimes, such as the GDPR, are designed for systems in which data is centrally collected, stored, and processed. Yet, blockchains decentralise each of these processes.

The GDPR does not provide clear rules on how to apply its principles to this emerging and disruptive technology. For instance, identifying who the data controllers and processors are, and what their respective responsibilities entail, is very challenging, particularly for protocol developers and for actors running the protocol.

The level of concern also depends on whether the blockchain is open or private. Compliance with the GDPR appears to be much more complex in the case of public ('permissionless') blockchains, whereas many industrial distributed ledger technologies (DLT) are more centralised, and thus less problematic.

Issue #2: Anonymisation of personal data

Another open issue concerns the anonymisation of personal data, that is, a process in which data cannot be traced back to any person. Blockchain networks rely heavily on the persistence of data over time, requiring its anonymisation for ensuring the privacy of all users.

Yet, there are still many debates as to which anonymisation techniques are more adequate and in line with GDPR rules. For instance, can these techniques truly make anonymisation irreversible?

Issue #3: Conflicting core principles and rights

Several core principles and rights of users, strengthened by the GDPR, appear to be in direct conflict with the functioning of a blockchain. The right to erasure, and the principle of data minimisation (i.e., for organisations to not hold more personal data than is actually needed) can be in conflict with the immutability (i.e., the unchangeable nature) of the information on a blockchain.

Nonetheless, experts argue that the extent to which a data subject is entitled to have their personal data erased is not an absolute right, and applies when the data subjects withdraw their consent on which the processing is based. Also, the legal definition of what 'erasure' means, and the extent to which obfuscation (making data unintelligible) by means of advanced cryptography, can be considered as erasure remain unclear. Several national regulators, such as the French *Commission nationale de l'informatique et des libertés* (CNIL), appear now to favour the use of such imperfect methods to improve interoperability.

Introduced by the GDPR, the right to be forgotten also appears to be in direct conflict with one of the core principles of blockchain: Transactions should be visible to all nodes in the network. Even the individual's right to access information regarding the processing of their personal data can be significantly limited by the fact that there is no clear data controller identified.

The way forward

As indicated in the EU Blockchain Forum's report, the GDPR and blockchain are not inherently incompatible. It is rather the lack of precise rules which can ensure GDPR compliance that is the most problematic.

European regulators and companies are yet to come forward with proposals that would both allow for the growth of blockchain innovation in Europe, while ensuring the protection of personal data for citizens. Experts have already developed scenarios which could guarantee GDPR compliance. For instance, they argue that when individuals interact with applications using public, permissionless, blockchains as backend, such as a cryptocurrency intermediary providing smart contracts, it is the owners of the application who could be considered the data controllers.

CNIL also recently unveiled its first analysis on the compliance of blockchain with GDPR, and indicated that blockchain was not adapted to all types of processing, with some being more relevant and potentially GDPR-compliant than others. For instance, the GDPR has strict conditions for allowing the transfer of personal data to third countries.

As a result, public blockchains seem particularly unfit since it can be very challenging to exercise control over where the users/miners are; private ('permissioned') blockchains can more easily provide solutions for controlling data flows to third countries. For open blockchains to comply with the GDPR, new types of blockchains, not carrying personal data, might need to be developed.

Technology can evolve to comply with privacy laws, but this will require extensive collaboration between regulators and companies.

CYBERSECURITY RESOLUTIONS TACKLED BY FIRST COMMITTEE

Two new resolutions on cybersecurity issues have been introduced by USA and Russia in the First Committee of the UN General Assembly, the committee dealing with disarmament and international security. We take a look at both drafts and the changes they have already undergone.

Developments in the field of information and telecommunications in the context of international security

Russia's proposed resolution, supported by 26 other countries, has undergone quite a few changes since it was introduced in the First Committee in mid-October.

The original draft included both a number of provisions from the country's draft Code of Conduct developed by the Shanghai Cooperation Organisation (SCO), and provisions from the 2013 and 2015 UN GGE reports. In addition, it included language that referred to a 1981 resolution (UN GA Resolution 36/103), related to the rights of states to combat dissemination of 'false or distorted news' which interfere with internal affairs, and the duty of states to abstain from 'defamatory campaigns, vilification or hostile propaganda' for interference with internal affairs. This additional language was highly disputed by some countries, who consider it provides a space for the violation of human rights and freedoms.

After rounds of negotiations, most of the language lifted from the SCO's Code of Conduct – such as the references to states not exploiting their dominant (technology) position, the protection of public order and morals, multilateral Internet governance mechanisms, curbing the dissemination of information that incites terrorism or hate speech, and states' control of goods and services – were removed from the draft.

The draft, however, maintained selected provisions from the UN GGE's reports – both in preamble and in recommendations – including the emphasis on sovereignty and non-intervention in international affairs, and jurisdiction of states over ICT in their territory (which are disputed by the USA and its allies), but also provisions related to respect for human rights and freedoms, reaffirmation that international law and the UN Charter are applicable, and recognition of the importance of the involvement of other stakeholders in the process. The selected provisions from the GGE reports also include those related to the duty of states to substantiate accusations of other states for attacks, the security of supply change, not attacking critical infrastructure or computer emergency response teams (CERTs), as well as the importance of sharing of vulnerabilities.

The draft resolution calls for the establishment an open-ended working group – rather than a new GGE – which would involve all interested states, allow possible inputs by other stakeholders, and report to the Secretary-General. The suggested mandate is, on a consensus basis, to further develop norms (short)listed in the draft resolution, discuss their implementation, discuss models for 'regular institutional dialogue with broad participation' under the UN, and hold 'intersessional consultative meetings' with other stakeholders.

Advancing responsible state behaviour in cyberspace in the context of international security

The USA's draft resolution, supported by 35 countries, underlines the work of the previous UN GGEs (2010, 2013, and 2015). It calls for the establishment of another GGE, mandated to further study norms, confidence-building measures (CBMs) and capacity-building measures, taking into account effective implementation of those, particularly suggesting that the report should contain written national submissions on how international law applies to cyberspace.

In addition, and unlike in previous years, the resolution invites the UN GGE chair to organise two open-ended informal consultative meetings, to allow states that are not members of the GGE (interestingly, other stakeholders were not mentioned) to share their views among themselves and with the chair (yet not with the GGE itself), who would then convey the messages to the GGE. The draft further invites the Office for Disarmament Affairs of the Secretariat to collaborate with regional organisations – namely the African Union (AU), EU, Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN) Regional Forum – to organise consultations on the work of the GGE, and feed inputs into its work.

While negotiations continue, the time available to reach consensus is shrinking. Voting on the draft resolutions is expected to take place in early November.

THE GIP AT THE 13TH INTERNET GOVERNANCE FORUM

The GIP will participate actively at the 13th IGF, in Paris and online. Join us for the following activities, and stay tuned for just-in-time session reports and IGF Daily summaries.

Read our *just-in-time reports*

The *GIP Digital Watch* observatory will provide just-in-time session reports from the IGF, and *IGF Daily* newsletters, which will be available on the dedicated webpage **dig.watch/igf2018**. A final report, published after the IGF meeting, will include a thematic summary. These will complement the dynamic updates offered through the observatory.

Join our *sessions*

The GIP is co-organising the following sessions:

The challenges of capacity development: a practical approach (WS #262) - Monday, 12th November - 10:10 to 11:10 - Salle VII

The need for capacity development in Internet governance and digital policy is voiced substantively and regularly in official speeches and documents. Experienced facilitators and consultants are active in this area. However, supply and demand do not always match. What does capacity development need to look like? What is the learning of activities on capacity development that could be useful to newcomers? Are there particular opportunities, risks, and benefits associated with capacity development in coming years?

AI and the future of diplomacy: What's in store? (WS #423) - Tuesday, 13th November - 15:00 to 16:30 - Salle VII

AI is under continuous evolution. We see it in various applications, from translation tools to self-driving cars and beyond. There are more and more discussions around AI, and the opportunities and challenges it brings to various sectors. These discussions range from fact to fiction and from dystopian views to practical interpretations. But the technology is here to stay and it will continue to influence all aspects of society. The session will build on three main themes: AI and the international geopolitical environment, AI as a topic on the international agenda, and AI as a tool for diplomacy.

Visit us at *our booth*

The GIP and DiploFoundation will have a booth at the IGF Village. Visit us to get your copies of the *IGF Daily* newsletter, this newsletter in print, and other digital policy-related publications.