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 SEPTEMBER

1. Stepping up cyber offensive capabilities

In recent years, countries have been stepping up their cyber operations. Our analysis shows that at least 30 countries have been actively pursuing offensive operations.

In September, Britain and the USA both stepped up their efforts. Britain announced the creation of a £250 million joint cyber force between its Ministry of Defence and the government's intelligence arm, the Government Communications Headquarters (GCHQ). The unit will be staffed by 2000 personnel recruited from the military and security services industry.

Across the pond, the USA released two cyber strategies in which it advances a more aggressive stance against malicious cyber activity, and positions its economic and security interests very closely together.

The first is the White House's first cybersecurity strategy in 15 years, which outlines forms of international co-operation (such as the role of stakeholders on an 'equal footing') and the close interplay between the economy and security (not only does the strategy specify this, but it emerges clearly around issues such as data flows and theft of trade secrets), and introduces a new Cyber Deterrence initiative.

Taking a more forceful stance is the US Department of Defense (DoD) new cyber strategy, which departs significantly from the previous 2015 strategy. Calling for the military to 'defend forward' (construed by a former US Cyber Command officer as active defense plus, implying the use of operations on non-US networks to stop threats before they reach their targets), it is less risk-averse than the previous strategy. It also refers to the private sector as the military's 'trusted' partner.

Additionally, the White House confirmed that it has reversed Presidential Policy Directive 20, which stipulated that a complex interagency process must be followed before deploying cyber weapons. Together with the fact that the Cyber Command was elevated to a Unified Combatant Command last May 2018, the new (classified) rules will give the DoD more flexibility and will effectively enable offensive cyber operations through the relevant departments.

Trends continue on page 3

UNGA 73rd GENERAL DEBATE
Speeches during the general debate reiterate countries' policy priorities – including those on digital policy. Backed by data analysis, we summarise the issues.
More on pages 7–8. *Credit: UN Photo/Loey Felipe*

Issue no. 34 of the *Digital Watch* newsletter, published on 2 October 2018, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Cedric Amon, Stephanie Borg Psaila, Amrita Choudhury, Andrijana Gavrilović, Stefania Grottola, Đorđe Jančić, Marco Lotti, Clement Perardnaud, Natasa Perućica | Design by Viktor Mijatović, layout by Aleksandar Nedeljkov, Diplo's CreativeLab | In addition to the *Digital Watch* newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (https://dig.watch) and join discussions on the last Tuesday of every month online, or at the GIP (https://dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu | Download your copy at https://dig.watch/newsletter/september2018

DIGITAL DEVELOPMENTS IN GENEVA

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

Cyberstability Conference: Preventing and Mitigating Conflict

The conference, on 26 September, organised by the United Nations Institute for Disarmament Research (UNIDIR) at the Palais des Nations, tackled a broad range of cyber-conflict-related issues. Some of the issues, such as the roles and responsibilities of states and the private sector, and Russia's new resolution (one of two proposed drafts) on norms of state behaviour in cyberspace, triggered a lively debate. Structured around four panels, the first explored the risk of conflict through malicious use of ICT. The panellists mentioned the difficulty of agreeing to universal standards and the risks that this uncertainty poses for states and the commercial sector alike.

The second panel focused on regional mechanisms and solutions for the prevention of cyber conflict. Stressing that regional approaches need to be specific to the area of the world where they are implemented, the speakers shared best cases from the African Union, the Asia-Pacific region, the EU, and the OECD. The third panel focused on the role of the private sector in countering the proliferation of ICT capabilities. Panellists from the private sector and academia presented different techniques, ranging from naming and shaming practices, to insurance markets and trade incentives.

The final panel discussed multilateral processes across initiatives. Many of the panellists reiterated the importance of finding a common agreement on the applicability of international law in cyberspace and the application of UN GGE recommendations.

Human Rights Council (HRC), 39th Session

During the 39th session of the Human Rights Council (from 10 to 28 September), several reports were considered, including the report of the High Commissioner of Human Rights on the right to privacy. Building on discussions held during the expert workshop in February, the report states that the right to privacy is not limited to private spaces, such as someone's home, but extends to public spaces and to publicly available information. It warns against intrusive practices that use technology to limit people's privacy both online and offline, and affirms that the international human rights frameworks offers a solid foundation for addressing challenges arising in the digital age. With regard to the responsibilities of the private sector, it refers to the UN Guiding Principles on Business and Human Rights (in particular, Pillar II) as an 'authoritative blueprint for all enterprises, regardless of their size, sector, operational context, ownership and structure, for preventing and addressing all adverse human rights impacts, including the right to privacy'.

Confidentiality of communication and privacy of data in the digital age (HRC side event)

This side event to the 39th session of the Human Rights Council, on 25 September, was organised by Privacy International and the International Network of Civil Liberties Organizations, with the support of the governments of Austria, Brazil, Liechtenstein, Mexico, and Germany. The event focused on recent developments at international and national level with regard to the protection of the confidentiality of communications and of personal data. The event represented a platform for sharing the findings of the following studies: the report of the United Nations High Commissioner for Human Rights on 'The right to privacy in the digital age', the report produced by the International Network of Civil Liberties Organizations 'Unanswered Questions: International Information Sharing', and the report on policy engagement for data protection 'The Keys to Data Protection' produced by Privacy International. In addition, the panel discussion addressed the question of data protection principles; the protection and implementation of privacy and data protection with regard to the collection and use of biometric data; and the implications for privacy of use and implementation of AI.

New technologies and human rights (HRC side event)

In another side event on digital issues, on 26 September, organised by the United Nations Research Institute for Social Development (UNRISD) together with the Permanent Missions of the Republic of Korea, Austria, and Denmark, the discussion looked at whether we can leverage technology as a catalyst for the improvement of the human condition, namely reducing existing inequalities and helping us maximise our opportunities. The speakers warned that technology tends to replicate existing inequalities and power imbalances as technology is 'like a frame: it shows the world as it exists but it is up to us to use it for good change'. Moreover, the speakers also considered that technology poses some limitations to human rights when it comes to ensuring the accountability and transparency of a device's functions. Hence, most of the speakers stressed the importance of carefully considering potential human rights fallout before a given technology is put on the market; the need to develop a multistakeholder approach while testing a device, in order to limit human rights violations; and the importance of considering embedding privacy in the design of the device (privacy by design).

DIGITAL POLICY TRENDS IN SEPTEMBER

Continued from page 1

2. Data localisation discussions intensify (again)

Discussions on data localisation intensified in September, largely due to a debate on the new e-commerce draft legislation in India, published during the summer. The bill has been controversial due to its data localisation provisions, which require online retail firms to store user data in India, and to the provisions aimed at curbing deep discounting practices (discounts which are abnormally high) which are being criticised by foreign companies who have invested heavily in the country.

This month, the Indian government announced a review of the bill, and formed a new group to address stakeholders' concerns over the draft policy.

In recent years, arguments around data governance have been quite polarised. Those in favour of data flowing freely across borders argue that that this fosters economic growth and is part of the foundation of emerging technologies such as artificial intelligence (AI). Most of the limitations are therefore unjustified and harmful. Yet, those who argue that data should stay within borders often highlight that the right to privacy can only be ensured if the data is localised, and that issues of lawful access to data would be facilitated if so. *Read more on page 6.*

In debates this month, discussions continued to follow this trend. The search for solutions employing a balanced approach to data governance, or to find some elements for common ground, continue.

3. Calls made for strengthening digital co-operation

At this year's UN General Assembly debate, digital issues were more prominent compared to last year's debate. *Read our analysis on pages 7–8.*

Several heads of states called for closer international cooperation aimed to deal with digital technology as an amplifier of both opportunities and risks for modern society. France reiterated that we need to establish contemporary rules 'that will make it possible to reconcile the development of AI with our ethical rules'. Qatar proposed hosting a conference to discuss an international instrument on cybersecurity.

Switzerland proposed Geneva 'as a platform for dialogue on new challenges at the interface between politics, society, innovation, science, and economy'. The UK referred to the need for global cooperation to set and enforce fair rules on trade, tax, and the sharing of data.

As a response for the growing calls for digital cooperation, the UN Secretary-General established the High-Level Panel on Digital Cooperation in July with the aim of finding ways and means to deal with digital challenges. The Panel held the first meeting in New York (24-25 September) which set the stage for worldwide consultations on values, principles, and modalities of digital cooperation on issues such as human rights and human agency, inclusive economy, and data governance.' The Panel will hold the second face-to-face meeting in late January. It will produce its report by May 2019.

The busy digital week in New York was also marked by the launch of Microsoft's Digital Peace campaign (on 24 September) which will gather support and signatures for a more secure cyberspace. Microsoft's latest initiative aims to encourage governments, industry, civil society, and individuals to work towards cybersecurity and cyber peace. This initiative, and other new proposals, are expected to be discussed during November's Paris Peace Forum and the Internet Governance Forum.

Credit: Manuel Geissinger from Pexels

DIGITAL POLICY: DEVELOPMENTS IN SEPTEMBER

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

The new UN High-level Panel on Digital Cooperation continued to discuss digital policy mechanisms with actors worldwide. The panel's focus areas will include, among other issues, building the capacity of individuals, organisations, and governments to adapt to the digital age; putting human rights and human agency at the centre of technology; and bridging the digital divide.

Sustainable development

same relevance

The International Telecommunications Union (ITU) and UN Women, in collaboration with the African Union Commission have launched a new initiative to equip girls and young women in Africa with digital literacy skills.

In its latest annual report, The State of Broadband: Broadband Catalyzing Sustainable Development, the Broadband Commission for Sustainable Development revealed that a growing number of governments have started to benchmark the status of broadband in their national plans, while raising concerns about the growing inequalities in access to broadband. The report also cites the rapidly expanding use of digital finance services – currently at 15.8% of the global population and anticipated to increase to 40% of the global population by 2025.

Security

increasing relevance

The USA has published its first cybersecurity strategy in 15 years. Meanwhile, the DoD published a summary of its new cyber strategy, which calls on the military to 'defend forward' and to disrupt cyber activity at its source.

The European Commission has proposed new rules to help ensure terrorist content online is swiftly removed. The new rules state that content must be taken down by Internet platforms within one hour of being notified by the national competent authorities. They will also be required to take proactive measures to protect their platforms and users from terrorist abuse.

The data of around 130 million clients of the Huazhu Hotels Group in China was being sold on the Dark Web for 8 bitcoins – a low amount for the 141.5 GB database which contains 240 million records of personal data.

E-commerce & Internet economy

increasing relevance

The European Commission released a concept paper on the modernisation of the World Trade Organization (WTO). The release comes a few days after the delivery of Commission President Jean-Claude Juncker's final State of the European Union Speech, in which he highlighted the need to tackle threats to multilateralism and engage in the reform of the WTO.

China announced a multi-billion dollar investment to develop the digital economy over the next five years, investing in projects on big data, the IoT, cloud computing, smart cities, and the digital Silk Road.

The Indian government announced a review of its recently published draft e-commerce policy, following criticism from stakeholders, in particular from the business sector. It has formed a new group to address stakeholders' concerns over the draft policy.

Amazon's total market value surpassed $1 trillion, making it the second American company to achieve this milestone, following Apple in August this year.

Digital rights

increasing relevance

The European Court of Human Rights ruled that Tempora, the UK's programme of mass surveillance, revealed by whistleblower Edward Snowden, violated the right to privacy of those targeted.

In their statement at the end of the Five Country Ministerial of 2018, the Five Eyes jurisdictions called on tech companies to voluntarily establish lawful access solutions to private data.

In Luxembourg, the Court of Justice of the European Union heard more than 70 submissions in seven hours of hearings as part of the legal case involving Google, the French data protection authority (known as CNIL), and the right to be de-listed. CNIL argues that EU citizens' rights are not respected; Google argues that 'the EU shouldn't impose its view on others'.

Jurisdiction & legal issues

increasing relevance

The European Parliament approved amendments to the EU Copyright Directive, which attempts to harmonise aspects of copyright law across the EU. The vote included two controversial points, enshrined in Articles 11 and 13, dubbed the 'link tax' (or 'snippet tax') and the 'upload filter', the essence of which has been largely retained in the amendments.

Infrastructure

same relevance

SACS, the new undersea cable connecting South America (Fortaleza, Brazil) to Sub-Saharan Africa (Luanda, Angola), has been activated.

Alphabet's project Loon reached a new milestone of providing Internet signal across 1000 kilometers. This is the farthest Loon has ever beamed Internet access. Alphabet is preparing to launch Loon as a commercial service in 2019.

Net neutrality

same relevance

California's approval of a new net neutrality bill, which prohibits blocking, slowing down websites, and anti-competitive zero-rating practices, was met by criticism from the head of the Federal Communications Commission ahead of the federal appeals court hearing.

New technologies (IoT, AI, etc.)

same relevance

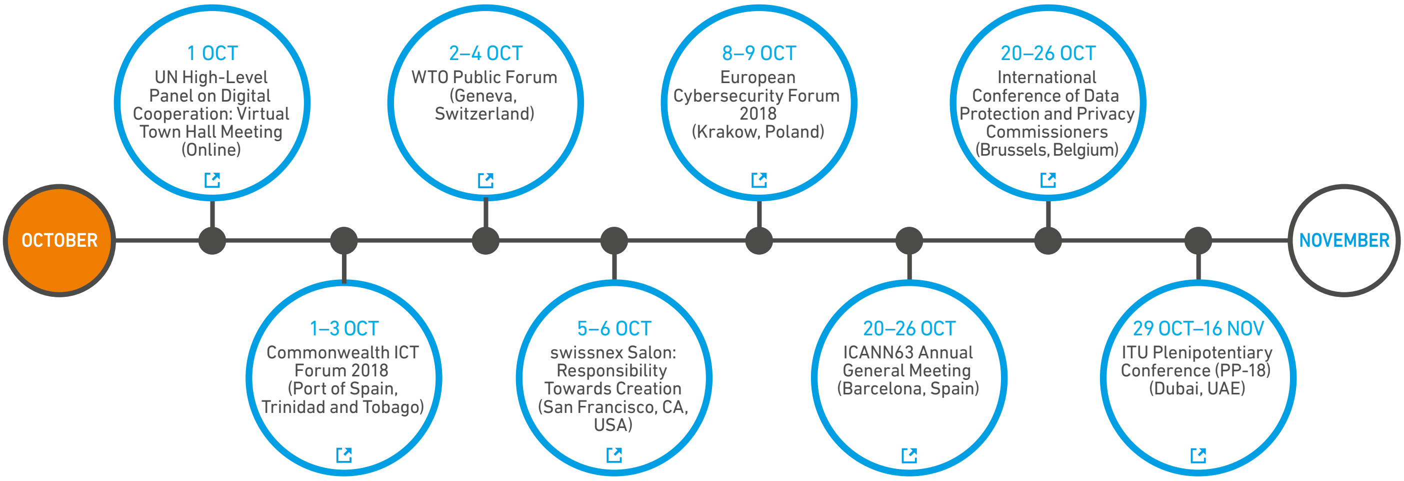
The European Parliament has called for an international ban on the development of lethal autonomous weapons systems, after some countries were reportedly developing them.

The US DoD's Defense Advanced Research Projects Agency (DARPA) has announced a multi-year investment of more than $2 billion in its AI Next artificial intelligence campaign. DARPA said that key areas to be explored will include automating critical DoD business processes, improving the robustness and reliability of AI systems, enhancing the security and resiliency of machine learning and AI technologies, and pioneering the next generation of AI algorithms and applications.

New research has explored the use of AI and machine learning for the healthcare industry, including in the development of pharmaceuticals, and in robotic surgery.

IBM plans to launch software designed to detect bias in AI models.

AHEAD IN OCTOBER



OCTOBER

1 OCT
UN High-Level Panel on Digital Cooperation: Virtual Town Hall Meeting (Online)

1–3 OCT
Commonwealth ICT Forum 2018 (Port of Spain, Trinidad and Tobago)

2–4 OCT
WTO Public Forum (Geneva, Switzerland)

5–6 OCT
swissnex Salon: Responsibility Towards Creation (San Francisco, CA, USA)

8–9 OCT
European Cybersecurity Forum 2018 (Krakow, Poland)

20–26 OCT
ICANN63 Annual General Meeting (Barcelona, Spain)

20–26 OCT
International Conference of Data Protection and Privacy Commissioners (Brussels, Belgium)

29 OCT–16 NOV
ITU Plenipotentiary Conference (PP-18) (Dubai, UAE)

NOVEMBER

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

IN PURSUIT OF DATA: THE MAIN POSITIONS ON DATA GOVERNANCE

Data is now recognised as an immensely valuable resource, with the potential to transform economies and societies around the world. As a consequence, control over data and its flows has become a strategic issue for a number of governments and companies, with diverging interests and competing agendas.

Many actors – among them a number of governments and the majority of companies – strongly support removing barriers to data flows to allow for the free flow of data across the Internet.

Others favour data localisation policies, aiming to restrict where data can be processed or stored. Inevitably, data localisation measures tend to fragment data flows.

What are the arguments in favour of the free flow of data and the localisation of data, in this crucial debate for the future of the Internet?

The free flow of data

The free flow of data is an essential condition for ensuring the speedy development of a data-driven economy. Data is the fuel of the digital economy. Progress in the fields of AI, machine-learning, and the IoT requires that data flows as freely as possible across national borders and jurisdictions. To deliver better results, these emerging technologies need an environment that is conducive to the free flow of data, in different sectors of our economies, such as agriculture, energy, environment, transport, and healthcare.

By definition, the proliferation of data localisation regulation poses the risk of a greater fragmentation of the open Internet and disrupts the seamless communication needed by new technologies. In the EU, several member states even argue that the free movement of data should be treated as a separate freedom of the EU together with the existing four freedoms of the internal market (goods, services, capital, and labour). This summer, the European bloc adopted rules that will allow data to be stored and processed everywhere in the EU without unjustified restrictions.

Some countries see data localisation measures as a non-tariff barrier to trade, and therefore a form of digital protectionism; often considered unjustified restrictions, these may impede the growth of the digital economy.

Restrictions on the storage and processing of data come at a high cost for businesses, amounting annually to billions of euro for EU companies according to the European Commission. These costs inevitably limit the competitiveness of businesses and their investments. Inversely, the free flow of data can generate new opportunities and foster innovation across borders.

Free flow of data clauses are increasingly being included in trade agreements, but with potential adverse consequences. Privacy advocates worry that this may provide third countries with the possibility to challenge comprehensive national data protection laws, disguised as a restriction on the free flow of data.

The localisation of data

Data localisation requirements usually concern the storage or the processing of data, and can be necessary for ensuring its access, privacy, and security.

The rise of cybercrime and cyber-threats brings serious challenges for governments worldwide, but the complexity of international rules seriously limits the ability of law enforcement agencies to access data stored in other jurisdictions. Data localisation measures can be thus seen by public authorities as a facilitator for accessing data in a timely manner.

Data localisation is also used as a mechanism to maximise data security, as shown by the case of the Chinese data localisation law. In response to revelations of US secret surveillance programs, a number of governments have indeed required 'critical' operators, including foreign companies, to store personal and sensitive data within their national territory, for security purposes.

Some actors view the EU's GDPR as an indirect form of data localisation, as it only allows for the flow of data to third countries if their legal systems comply with European rules. In this case, limitations to the free flow of data are justified by EU lawmakers by the necessity to protect the right to privacy of EU citizens. In addition to privacy protections, a large number of states have put in place restrictions to cross-border data flows, for taxation and security purposes.

The debate is expected to continue, as countries search for a formula for data governance that will balance the various rights and interests.

Credit: David Werbrouck on Unsplash

UN GENERAL ASSEMBLY'S ANNUAL DEBATE: THE STATE OF THE DIGITAL WORLD

Every third week of September, global attention shifts to the United Nations Assembly Hall. Heads of state descend upon New York to outline their countries' views on international issues, and to signal their diplomatic priorities for the next 12 months. Once again, we provide an analysis of the digital issues covered by the speeches.

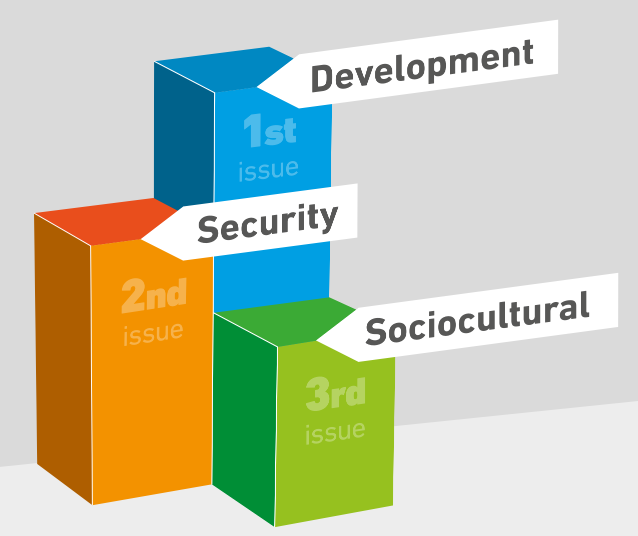
This year, the UN Secretary-General, António Guterres, set the tone by including digital issues alongside top priority issues such as climate change and crisis management. Trust – or rather, the lack of trust – provided the context for what is ailing today's world: what Guterres described as 'a bad case of "trust deficit disorder".

Trust is also diminishing in the digital sphere. The risk of weaponisation of artificial intelligence (AI), the growing misuse of technology by criminals, and the widening gender gap in digital access are some of the issues highlighted in the Secretary-General's speech, and in the work of the High-Level Panel on Digital Cooperation which he established in July. Yet, there was hope that things can be improved. In both the offline and online worlds, trust can be rebuilt.

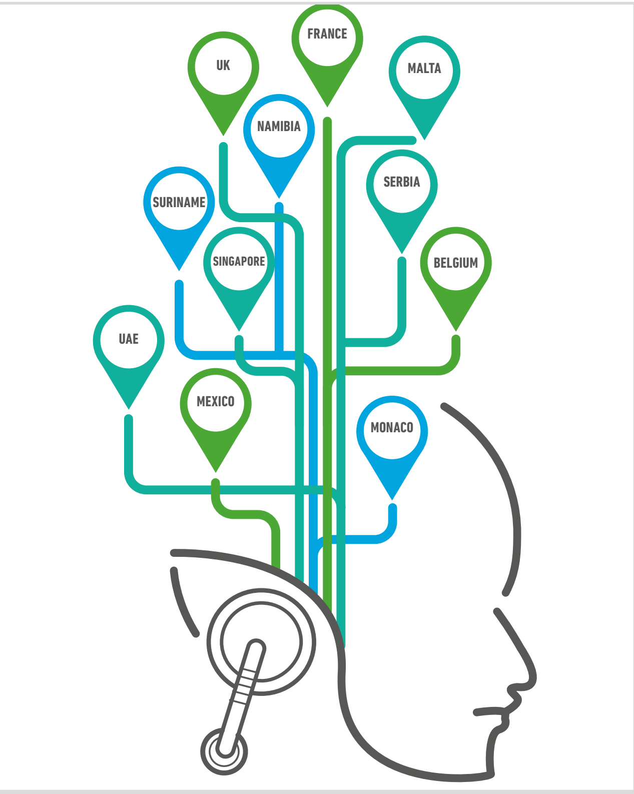
Most national statements which reflected on digital issues ranged between focusing on opportunities (digital technology as an engine of social and economic progress) and focusing on risks (digital technology as amplifying the risks for a secure modern society).

In comparison to last year's study, our analysis of this year's statements revealed the following trends and patterns:

1. Digital issues were increasingly prominent. A total of 63 statements, compared to last year's 47, tackled digital aspects. The coverage ranged from the simple mention of digital technology, to more in-depth elaboration of concrete proposals.
2. This year saw an increase in debates on digital risks, compared to the more positive digital opportunities which were predominant in last year's speeches. Cybercrime, violent extremism, and the risks posed by the uncontrolled growth of AI featured highly in the statements. A total of 20 heads of states raised specific concerns about security issues.



Our data analysis identified development-related issues as the most mentioned digital issue across the statements



A total of eleven countries referring to AI in their speeches

3. Regional differences were noticeable in the framing of digital risks and opportunities. Only ten African states mentioned digital aspects. Their main focus, rather, was on the potential of digital technology for economic growth and employment. Statements from Europe offered a more prominent coverage of the risks of digital developments. Reflections on more balanced risks and opportunities could be found in the speeches of heads of states from Asia and Latin America.
4. Lastly, there was the noticeable absence of digital coverage in the statements of two of the major digital powers, the USA and China. President Trump did not make any reference to digital issues, while Minister Wang Yi mentioned the matter only in the context of national security and the fight against terrorism.

Apart from digital aspects, the most of statements this year focused on the following:

- The state of multilateralism (the crisis, the risks, and 'negative multilateralism')
- Reform of the UN
- Unresolved crises (such as in Yemen, Syria, and Myanmar)
- Progress in crisis management (successes included the Djibouti Agreement between Eritrea, diplomatic relations between Ethiopia and Somalia, and the Singapore Summit between the USA and North Korea)
- Climate change (adherence to the 2015 Paris Agreement and the 2019 UN Climate summit)

Continued on page 8

Continued from page 7

- Migration (a mention of the Global Compact and Conference in Marrakech)
- Sustainable development

The issues in detail

Security aspects

In terms of security, most nations are concerned about rapidly growing cybercrime rates, the rise of small arms trade through digital platforms, and the spread of terrorism through digital means. In addition to these threats, the EU and other leaders of European countries mentioned dangers arising through misinformation as well as political interference and meddling in electoral processes.

Estonia and Slovakia warned against the risk of underestimating digital security risks. Slovakian president Andrej Kiska said that malicious activities in cyberspace are 'as dangerous as any conventional threat'.

Russia reiterated its plans to propose two draft resolutions; one regarding the responsible behaviour of states in cyberspace as well as a draft resolution for a universal convention on countering cybercrime. Cuba warned against the militarisation of cyberspace and condemned the illegal use of new technologies to attack other countries.

Infrastructure and economic aspects

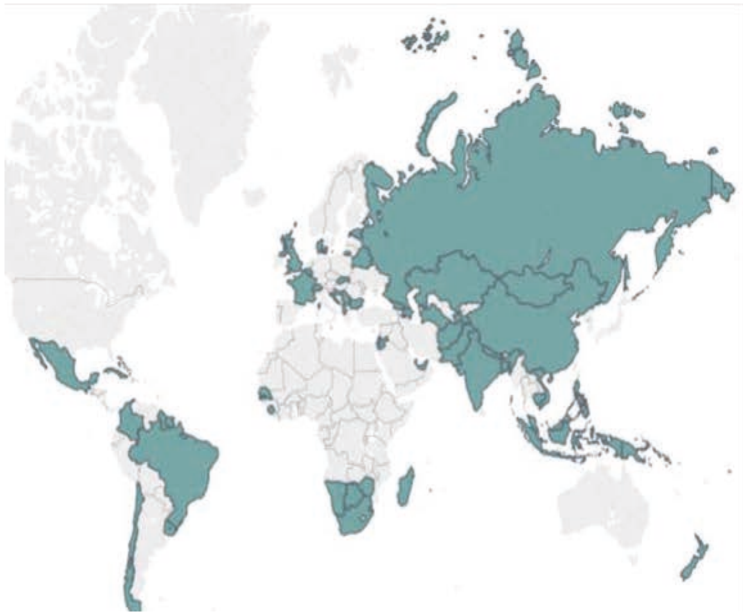
Challenges mentioned by the members of the UN General Assembly also referred to disruption of labour markets through digital technologies and challenges faced by younger populations in relationship to these disruptions (Croatia). In light of these developments, the Secretary-General said: 'Governments may have to consider stronger social safety net programmes, including, possibly, universal basic income.'

Malta referred to the major digital opportunities: from advanced robotics and AI, to 3D printing and the Internet of Things. States should prepare for, and embrace, the new changes of this age. The sentiment was echoed by India, as well as by different African countries such as Namibia, Botswana, the Kingdom of Eswatini (formerly known as Swaziland), and Sierra Leone, who spoke about their investments in the digital economy as a promising avenue for growth.

The unsaid

This year again, the silence and absence of statements regarding digital issues were noteworthy. While China only briefly alluded to the topic of cybersecurity and the fight against online terrorism, the USA avoided the topic entirely. From the US side, this is an interesting trend as it follows last year's speech during which President Trump only referred to 'new forms of aggression exploit[ing] technology to menace our citizens'.

Brazil, which was previously more outspoken about digital issues and had left out this topic in 2017, only alluded to digital topics. President Temer mentioned the role and importance of new technologies in the context of international trade and cross-border flows.



Mapping the countries' statements

Our map compares the references to digital issues with last year's statements, and provides an in-depth coverage of the digital-related issues mentioned by the countries.

View the interactive version at *dig.watch/unga73*

List of countries
(All) ▾

Reference to digital issues in 2017
(All) ▾

Reference to digital issues in 2018
Yes ▾

□ (All)
□ No
☑ Yes