Newsletter

Clamping down: Internet shutdowns on the rise

TRENDS IN JULY & AUGUST

Privacy investigations are on the rise, Internet access is disrupted in many regions, and AI developments continue at full speed.

More on pages 2–3

FROM THE OBSERVATORY

Sustainable development, digital rights, and new technologies were the most prominent issues in recent weeks. Why were they important?

More on pages 4–5

IN FOCUS: FACIAL RECOGNITION

The use of facial recognition technologies generates growing concerns over human rights implications.

More on pages 6

DIGITAL GOVERNANCE

In an increasingly digitalised world, who and how should respond to calls for solutions to digital policy challenges?

More on pages 7

The top digital policy trends in July & August

Every month, we analyse hundreds of developments to identify the trends in digital policy and the unfolding issues that drive it forward. These are the key trends that sum up the months of July and August.

1. Privacy and data protection investigations increase

Stronger privacy regulations have been put in place in recent years, imposing strict requirements for companies that process personal data. The EU General Data Protection Regulation (GDPR) has become somewhat of a global standard, with many countries adopting similar rules. But data breaches and privacy violations continue to happen, leading to an increase in the number of investigations launched by data protection authorities (DPAs) around the world.

In Ireland, the Data Protection Commissioner opened the third privacy investigation into Apple's compliance with the GDPR. In the UK, the Information Commissioner's Office is investigating video sharing app TikTok over its compliance with children's privacy rights, and looking into a potential misuse of personal data by the face-editing photo app FaceApp. These are only some recent examples.

Internet of Things (IoT) companies have also attracted their share of investigations, with smart speakers and assistants in the spotlight. The DPA in Hamburg, Germany, ordered Google to stop using data collected from its smart speakers, following revelations that some company employees and contractors had access to extracts of users' conversations. Luxembourg's National Data Protection Commission is discussing concerns over recordings of user's everyday conversations made by Amazon's Alexa. Apple's Siri was also subject to similar concerns recently, leading the company to stop the practice of allowing contractors to listen to Siri recordings to 'grade' them.

In addition to launching new investigations, authorities have started to impose heftier fines on companies breaching privacy rules, the most prominent of which was the Facebook/US Federal Trade Commission (FTC) settlement for US$5 billion in the Cambridge Analytica case. The FTC also reached a US$700 million settlement with Equifax over a 2017 data breach, as well as a multi-million dollar settlement with YouTube over violations of children's privacy laws. In the UK, British Airways was fined €183 million for GDPR violations. But many wonder whether these fines and settlements are substantive enough to make companies improve their privacy practices.

The Court of Justice of the European Union (CJEU) continues to be busy with data protection cases, including its recent ruling requiring websites using Facebook's 'Like' buttons to warn users about the collection and processing of personal data.

What do all these privacy investigations and court cases signal? There is certainly increased pressure on companies to place more importance on protecting their users' rights to privacy and data protection. It may also be a sign that users themselves are paying more attention to what happens with their data once it is in the hands of private companies.

What remains to be seen is to what extent companies will adapt their data-processing practices as a consequence of the fines imposed by DPAs and the rulings issued by courts.

2. Internet access disrupted in many regions

Many of us take the Internet for granted and rarely think about what would happen if we were disconnected. But Internet access disruptions are a reality in many regions, where it is a common practice for authorities to impose Internet shutdown measures when confronted with political crises and citizen protests. These measures vary from blocking access to social media platforms and messaging services to complete Internet blackouts.

In August, disruptions were recorded in the Kashmir region, in Algeria, and Russia. Indonesia was urged to end Internet shutdowns in the Papua and West Papua provinces, while the Ethiopian prime minister defended the recent shutdowns.

This alarming trend of governments blocking access in an attempt to tackle social unrest has prompted intense criticism. Human rights advocates argue that Internet restrictions breach the individual's right to information, freedom of expression, and freedom of assembly, and that they often lead to increased violence.

Read more in our special section on pages 8-9: Data Analysis: Mapping Internet shutdowns and their implications.

3. AI developments continue at full speed

Artificial intelligence (AI) is a fast-evolving field as tech companies and scientists continue to develop new AI applications. One prominent area is biology, where several AI developments over the past two months illustrate a new trend.

Scientists at Flinders University in Australia have developed a flu vaccine thanks to AI, while in a Facebook-funded study, neuroscientists at the University of California in San Francisco found a new way to decode speech directly from the human brain, using machine learning in the process. Elon Musk's company Neuralink revealed some of its work on brain-machine interfaces (BMIs), promising progress in enabling direct communication between the brain and external devices, such as artificial limbs. Google presented details of its work on impaired speech recognition and hand-tracking technology, showing progress in both fields.

While new developments are exciting, innovation in AI is also triggering concerns. How far would BMIs go, for example? Do we want machines to be able to read our minds? If so, what would this mean for humanity?

While BMIs remain very much an area of ongoing research, facial recognition technology is already in use and continues to attract controversy. Over the past two months, new bans were imposed on the use of this technology, lawsuits were launched, and concerns about privacy rights and the risks of bias resurfaced. *We analyse this in more detail on page 6: Facial recognition: To trust or not to trust?*

On the policy side, countries continue to work on national AI strategies and plans, though at a slower pace compared to previous months. In the EU, several member states (e.g. Croatia, Cyprus, Hungary, Slovenia, and Spain) need more time to develop their AI strategies, although the European Commission had recommended that they do so by mid-2019. *Test your knowledge on AI strategies with our crossword on page 12.*

Meanwhile, the incoming president of the European Commission announced plans to develop 'legislation for a coordinated European approach on the human and ethical implications of AI'. It will be interesting to see what this legislation will mean for EU countries and tech companies, as the EU tries to achieve a balance between encouraging AI research and development and ensuring that progress in this field is in line with European values.

Credit: Ars Electronica, Tom Mesic

Digital policy developments in July & August

With so many developments taking place every week, the policy environment is chock-full of new initiatives, evolving regulatory frameworks, new court cases and judgments, and a rich geo-political environment.

Through the *Digital Watch* observatory, we decode, contextualise, and analyse these issues, and present them in digestible formats. The monthly barometer tracks and compares them to reveal new focal trends and to determine the presence of new issues in comparison to the previous month. The following is a summarised version; read more about each one by following the blue icons, or by visiting the Updates section on the observatory.

same relevance

Global IG architecture
The G20 leaders' Osaka Declaration on Digital Economy has sparked intensified discussions on facilitating cross-border data flows with trust.

G7 leaders have agreed on the Biarritz Strategy for an open, free, and secure digital transformation, outlining commitments in areas such as cross-border data flows and AI.

increasing relevance

Sustainable development
The High-level Political Forum on Sustainable Development concluded its annual meeting dedicated to reviewing six sustainable development goals (SDGs). Among the 100+ statements delivered by state officials, 53 referred to technology, including its role in attaining the SDGs.

The Economic and Social Council (ECOSOC) adopted a resolution on the role of frontier technologies in fulfilling the SDGs. A set of Best Practice Guidelines on fast-forwarding digital connectivity for all was adopted during the Global Symposium for Regulators organised by the International Telecommunication Union (ITU).

same relevance

Security
Microsoft revealed that nearly 10 000 of its customers were targeted or compromised by nation state cyber-attacks in 2018. The US National Security Agency announced that it will create a new Cybersecurity Directorate to prevent and eradicate foreign cyber threats. The UN Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (UN GGE) held regional consultations with the Organization of American States.

The African Union has called for more efforts to combat cyberterrorism. Cybersecurity Tech Accord signatories have agreed to implement vulnerability disclosure policies by the end of 2019. The UK's High Court ruled that the Investigatory Powers Act contains enough safeguards against the risk of abuse of the government's electronic surveillance power.

increasing relevance

E-commerce & Internet economy
USA and France have reached a compromise on the new French digital tax. France will repay tech companies the difference between the French tax and the tax to result from the taxation mechanism being developed by the Organization for Economic Cooperation and Development (OECD). G7 Finance Ministers adopted the Common Understanding on Competition and the Digital Economy, stating antitrust laws should adapt to the challenges of the digital economy. The UK's competition authority is considering measures to protect consumers against the growing power of technology giants. The Australian consumer and competition watchdog has issued recommendations for regulating digital platforms.

Facebook-owned WhatsApp plans to launch its first payment service in India in 2019. Facebook's Calibra head, David Markus, testified about Facebook's cryptocurrency plans in front of two US Congress committees.

Observatory

Digital rights

Tech companies face more privacy investigations, as a third investigation against Apple is launched in the UK, and Facebook CEO is questioned over child privacy protection in Kids Messenger app.

Facebook was fined an 'unprecedented' US$5 billion by USA's FTC over the Cambridge Analytica privacy breach.

China's National Computer Emergency Response Team has expressed concern over apps' over collection of users' data.

Car manufacturer Mercedes-Benz is involved in a privacy scandal over car trackers.

Internet access faces disruptions in many regions, including Kashmir, Indonesia, Algeria, and Russia. Previously imposed Internet restrictions were lifted in Sudan, Mauritania, and Chad.

increasing relevance

Jurisdiction & legal issues

The CJEU ruled that websites using Facebook' 'Like' buttons need to seek users' consent when collecting and processing personal data.

The US Appeals Court ruled that Facebook is not liable for terrorist content published on the platform. The company requires users to provide only basic information and therefore acts as a neutral intermediary.

Australia plans to block websites 'hosting harmful and extreme content from terrorists', the country's prime minister said.

increasing relevance

Infrastructure

New undersea cables link Australia to Papua New Guinea and the Solomon Islands and bring high-speed Internet to the two islands.

Huawei and Intel announced the launch of powerful AI chipsets.

The CJEU fined Belgium for failing to provide broadband Internet infrastructure in Brussels.

same relevance

Net neutrality

New research shows that Internet service providers (ISPs) are throttling online video traffic.

The US Federal Communications Commission (FCC) denied the claim that Verizon breached net neutrality rules in 2016.

decreasing relevance

New technologies (IoT, AI, etc.)

Scientists are pushing the boundaries of AI applications to develop flu vaccines, to decode speech from the human brain, and to improve speech recognition and hand-tracking technology.

Facial recognition technology faces new bans and investigations in the USA, the UK, and India.

Incoming European Commission president announced plans for legislation on ethical implications of AI.

Amazon will allocate US$ 700 million to provide a third of its employees with upskilling training programmes in new technologies.

increasing relevance

Facial recognition technology: To trust or not to trust?

Facial recognition technology (FRT) has been around for more than 40 years, but it is only in the past decade that we have seen an increase in its use by tech companies, law enforcement agencies (LEAs), airports, banks, etc. Despite its promises, FRT is generating growing concerns because of its human rights implications.

What is the technology used for?

In simple terms, FRT uses algorithms and machine learning to identify a human face from a photo or video. For example, FRT systems are used by LEAs to identify individuals by comparing their images with a database of known faces. In certain cases, such as Amazon's Rekognition, the technology is also able to recognise facial gestures, and even emotions such as fear and happiness.

What are the main concerns?

Like any other technology, FRT has its limitations and risks. A 2018 study showed that FRT programs developed by IBM, Microsoft, and Chinese company Face Plus Plus presented skin-type and gender biases, as the algorithms were largely trained on photos of males and white people. Amazon's Rekognition was also found to show racial and gender biases, and wrongly identify California lawmakers as criminals. The risk of bias and discrimination in decisions made based on FRT (e.g. false arrests) represents a key argument for those advocating against the use of FRT by authorities.

FRT also generates privacy concerns. Think of FRT-enabled street cameras: Are individuals aware of who uses their biometric data collected via such cameras and how they use it? How do authorities ensure that privacy rights are not breached? This is what the UK DPA is wondering, having opened an investigation into the use of FRT in street camera systems at King's Cross in London. Similar privacy concerns have recently been raised in India, when the Bengaluru and Hyderabad airports in India started experimenting with FRT, and in Sweden, whose DPA has imposed a €200 000 fine on a school for using FRT to monitor students' attendance. Beyond these examples, there is also the risk that, when used extensively by authorities, FRT could lead to mass surveillance.

Privacy concerns also apply to tech companies and their use of FRT. In August, a San Francisco court allowed the continuation of a class-action lawsuit against Facebook. In this case, users claim that the company is illegally processing biometric data to identify users in photos.

And so, can it be trusted?

If the technology poses such risks and limitations, can it be trusted? Several public and private entities do not seem to be very concerned about the dangers, as FRT is used or tested in countries such as the USA (across many cities), China, Japan, Singapore, and the United Arab Emirates.

But in Oakland, San Francisco, and Sommerville, in the USA, the use of FRT by LEAs is now banned. US presidential candidate Bernie Sanders shares a similar concern: If elected president in 2020, he will ban the use of facial recognition by the police.

Tech companies have also reacted differently. While Amazon refused to stop selling Rekognition to LEAs, Google said it would not sell general-purpose FRT before addressing tech and policy questions, while Microsoft has called for regulations to govern the use of the technology.

The likelihood is that companies will continue to develop and improve their FRT. What is less certain is whether future improvements will make the technology safe enough to address the concerns currently being raised by human rights advocates. At the moment, trust in FRT is hanging in the balance.
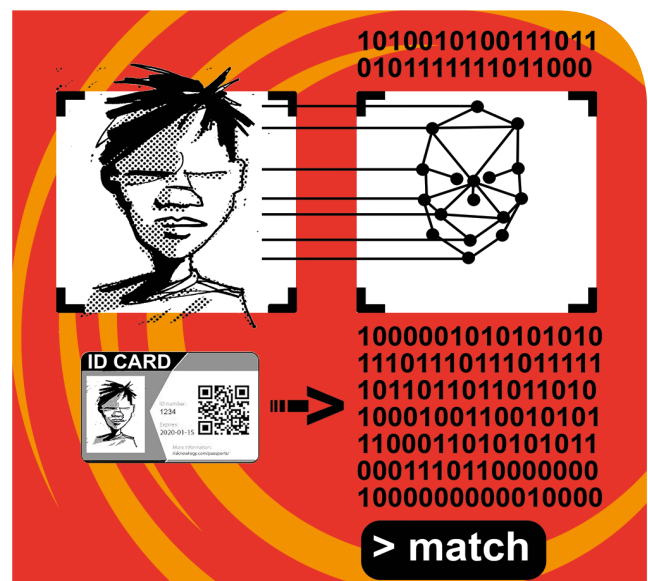
Digital governance: Responding to digital policy calls

The more digitalisation impacts our lives, the more citizens, companies, and countries call for digital policy solutions to issues in the fields of AI, e-commerce, fake news, and more. Who should address these calls and how? Where should responses be developed?

These questions were tackled by the High-Level Panel on Digital Cooperation established by the UN Secretary-General. Drawing on former US Secretary of State Henry Kissinger's famous question - Who do I call if I want to call Europe? - and adapting it to the digital realm, Dr Jovan Kurbalija, former Co-Executive Chair of the Panel's Secretariat, explained how the Panel tackled these questions in its final report.

Who should respond?

Effective policy solutions require the inclusive participation of governments, the tech industry, local communities, academia, and other actors.

All actors should participate according to their respective roles and responsibilities. At the risk of oversimplifying: governments' role is to adopt public policies; industry to provide technical solutions; and civil society to hold all actors accountable.

How should we respond?

1. Digital policy actions must be rapid. The traditional method of drafting treaties takes a long time. But this is not adequate for dealing with fast-evolving issues such as data governance, AI, cybersecurity, and e-commerce.

2. The cross-border nature of the Internet requires international policy solutions. For example, it is not easy to impose national taxes on global tech companies. Thus, the EU, the OECD, and the G7 are searching for international solutions to digital taxation.

In the context of international policy solutions, the UN has to find a new role as a 'digital home' for all nations and all people. Quite a few bricks have already been laid by the Internet Governance Forum (IGF). But the IGF needs to further evolve to deal with ongoing digital developments.

3. Digital governance must deal with many (un) known unknowns. It is difficult to predict the emergence of digital policy issues, or to prevent them. But we have to prepare to deal with their consequences. The Panel proposed policy sandboxes and incubators which can react fast to policy problems, and develop and adapt solutions accordingly.

4. Digital solutions require policy choices and trade-offs between different interests. Some of the most complex debates have pitted issues against each other, such as freedom of expression vs dealing with hate speech, and privacy vs the data-driven economy. To facilitate informed and effective trade-offs, the digital governance architecture should provide a space for reconciling different interests and positions.

5. Digital issues must be addressed in a multidisciplinary way. Dealing with data requires us to consider commercial, technical, security, and human rights policy issues. AI is about technology, but also about ethics, law, and security. Digital inclusion is about 'Internet cables', but also about affordability and skills. The list goes on. Almost all digital issues require multidisciplinary solutions.

Where should we respond?

Given the overall functionality and impact of the Internet, many digital policy issues require a global approach. The Panel proposed three governance models for addressing digital issues on the global level: IGF Plus, Distributed Co-Governance Architecture, and Digital Commons Architecture. Among them, the IGF Plus proposal is the most mature and closest to the digital reality. But all three models provide space for convergence among different views and positions. And, after many policy and academic discussions on digital discussion, it is now time for consolidation and action.

For details on the Panel's proposed governance model, read the full article: Digital governance: Who is picking up the phone? and also our summary, published in June's issue of this newsletter.

Internet shutdowns: Mapping Internet restrictions and their implications

Access to information, freedom of expression, and freedom of assembly are essential for democratic societies to function properly, and the Internet facilitates the exercise of these rights. But in recent years, Internet shutdowns have become a tool for suppressing dissent, and for restricting communications during times of unrest. What is the situation in 2019 and what are the costs and implications of Internet restrictions?

Internet shutdowns on the rise

In July and August, Internet shutdowns were prominent. A major Internet shutdown was registered in the crisis-laden Kashmir region. UN human rights experts described the measure as 'a form of collective punishment of the people' living there, and urged the Indian government to end the communication shutdown. Other Internet restrictions were reported in Algeria and Russia. Indonesia was urged to end Internet shutdowns in the Papua and West Papua provinces.

Despite being four months away from the end of the year, our data analysis is clear: There has been a sharp upward trend in partial and widespread Internet restrictions. Shutdowns are also lasting for a very long time. For instance, the Sudanese population was cut off from the virtual world for more than a month, while Chad faced the longest Internet shutdown ever recorded; it lasted for almost a year.

Mapping Internet shutdowns

Data from activist organisation AccessNow for 2016, 2017, and 2018 shows an increase in the number of Internet shutdowns. In 2016, 75 Internet outages were recorded, while in 2018 the number increased significantly, amounting to a total of 196 shutdowns.

This year, until August 2019, our research of shutdowns based on data from the *GIP Digital Watch* observatory, shows that 149 Internet shutdowns have been documented to date. With four months to go until the end of the year, the trend indicates that we may expect even more partial or full Internet shutdowns, possibly making 2019 the year with the most shutdowns ever recorded.

As to previous years, the highest number of Internet shutdowns was recorded in India (77 cases), followed by Venezuela (31). The high number of Internet restrictions in Venezuela in comparison to the previous years is attributed to the ongoing political crisis.

Note: Data for 2019 is from January to August

Shutdowns in numbers
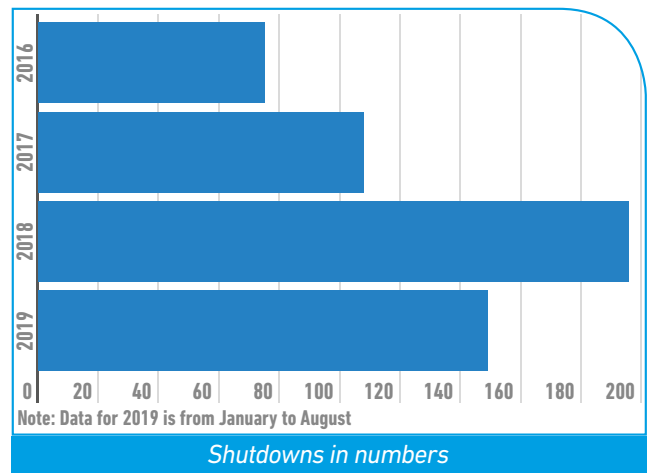
Our research shows that the vast majority of Internet shutdowns occur prior to, during, or after elections as well as during mass protests. However, examples from Algeria, Ethiopia, and Iraq also show that Internet restrictions are imposed during national school examinations.

A significant number of Internet outages were partial, given the targeting of particular websites and social media platforms, including Facebook, Twitter, and online streaming services such as YouTube.

Economic, political, and human rights implications

Internet disruptions cause serious economic damage to states where they occur. Aside from preventing businesses from conducting their daily activities, they also negatively impact foreign investments, employment, productivity, and sales.

A study conducted by the Brookings Institute approximated the annual cost of the Internet shutdowns worldwide at US$2.4 billion. In another study by NetBlocks and the Internet Society, the Cost of Shutdown tool shows that in Venezuela alone, a day without the Internet is valued at over US$400 million, whereas in India the loss is estimated to be around US$1 billion.

Data analysis

Even though Internet shutdowns are imposed under the pretext of maintaining stability and safeguarding national security, facts show otherwise. They are often used to mask political instability and dissent, thus leading to obstruction of democratic processes and isolation of certain regions.

Internet blackouts have grave direct and indirect consequences on fundamental human rights and freedoms. In 2016, the United Nations Human Rights Council unequivocally condemned 'measures to intentionally prevent or disrupt access to or dissemination of information online' and called on all states 'to refrain from and cease such measures'. ⬀

Clampdowns are frequently criticised by the international community. Recently, the UN Special Rapporteur on the situation of human rights in Myanmar, ⬀ Internet Without Borders, ⬀ the Committee to Protect Journalists, ⬀ and the USA, ⬀ among others, called on Myanmar, Benin, and Indonesia to restore Internet services.

Reacting to criticism

The Ethiopian prime minister defended the Internet shutdowns recently experienced by the country. The Internet, he said, is 'neither water nor air' and could be cut off forever if needed to curtail deadly unrests. ⬀

What is an Internet shutdown?
An Internet shutdown is an intentional disruption of the Internet or electronic communications, ⬀ making them inaccessible or effectively unusable. Emphasis is on 'intentional'.

Shutdowns can be nationwide, or target a location often to exert control over the flow of information. They can also be partial, where the outage refers to blocking certain websites and/or social media platforms, or a total Internet blackout, in which citizens are unable to access the Internet in its entirety.

Yet many restrictions also come to an end following pressure on governments, or rulings by the courts. For instance, in January, Zimbabwe's High Court ruled that the Internet shutdown was illegal and ordered the government to reconnect. ⬀ Internet access restrictions imposed in June in Sudan ⬀ and Mauritania ⬀ were lifted in early July. Chad's president has reportedly announced the restoration of access to social media platforms, after over a year of outage. ⬀

Follow the latest developments on access on the GIP Digital Watch observatory. ⬀

Number of Internet shutdowns per country in 2019
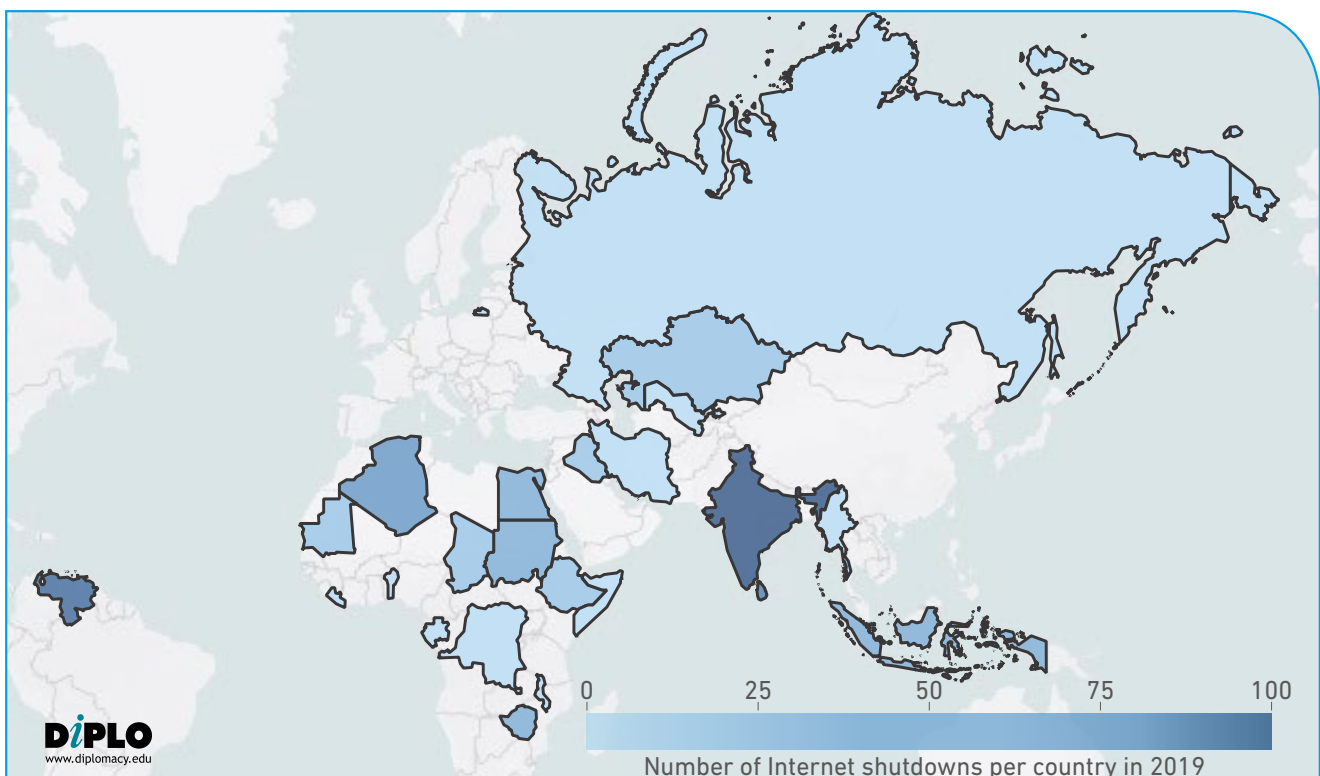
Policy discussions in Geneva

Numerous policy discussions take place in Geneva every month. The following updates cover the main events in July and August. For event reports, visit the *Past Events section on the GIP Digital Watch observatory.*

Human Rights and Digital Technologies: New Insights | 3 July 2019

Held as a side-event to the UN Human Rights Council, the session discussed the role of the Internet in fostering greater dialogue, empowering marginalised groups, and facilitating the exchange of information and ideas. Organised by the Geneva Academy of International Humanitarian Law and Human Rights, the Swiss Federal Department of Foreign Affairs, the United Nations Special Procedures of the Human Rights Council, and the Geneva Internet Platform, the session highlighted the need to address concerns about the degree of autonomy of new technologies and how this impacts human rights. Digital rights issues are now largely tackled inside traditional human rights circles such as UN bodies; actors must therefore take the discussions outside of these circles to ensure that human rights concerns are addressed appropriately.

Read our reports from the sessions.

Advancing digital and sustainable trade facilitation for trade diversification and inclusive development | 4 July 2019

How are countries progressing with implementing measures under the World Trade Organization's Trade Facilitation Agreement? How are economies implementing technology-driven measures to strengthen the use and exchange of electronic trade data? This event discussed the preliminary results of the 2019 Global Survey on Digital and Sustainable Trade Facilitation, which was conducted by the five UN regional commissions across 128 economies from 8 regions. The survey found that countries have generally made significant progress in trade facilitation. Yet more efforts are needed to enhance cross-border co-operation and interoperability among paperless trade systems, and to enable the safe and seamless flow of electronic data and documents in the framework of international supply chains.

2019 Innovations dialogue: Digital technologies and international security | 19 August 2019

The conference, organised by the United Nations Institute for Disarmament Research, discussed digital innovations and their impact on international security. Break-out sessions, led by practitioners from the tech sector, academia, and international organisations, looked at how quantum computing, distributed ledger technologies, and the IoT work. Discussions focused on the impact of AI on the prevention and de-escalation of conflicts, as well as on strategic decision-making. A key message was that more co-operation is needed among different stakeholders in addressing the security implications of new technologies.

Second meeting of the Group of Governmental Experts on LAWS | 20–21 August 2019

Following the first meeting of the Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems (LAWS) in April, the second meeting focused on finalising the group's 2019 report. On substantive issues, the group made progress by adopting the guiding principles affirmed in 2018, which include aspects such as the applicability of international humanitarian law (IHL) to all weapons systems, and the need to retain human responsibility for decisions on the use of weapons systems. The group identified an additional principle, which states that human-machine interaction should ensure that the potential use of LAWS is in compliance with applicable international law, in particular IHL. Contentious issues re-emerged, including those related to the group's mandate, as well as substantive issues related to human control and judgment in the use of LAWS.

The main global digital policy events in September

We look ahead at the digital policy calendar to highlight the main global discussions taking place in the next few weeks. For some of them, the observatory will provide reports from individual sessions and a final report summarising the discussions.

September

9–13 SEPTEMBER
First meeting of Open-Ended Working Group (New York)

The first substantive session of the Open-Ended Working Group (OEWG) on developments in the field of ICTs in the context of international security will be held on 9–13 September 2019. The task of the OEWG is to continue developing the rules, norms, and principles of responsible behaviour of states and discuss ways of implementing them, and to explore the possibility of establishing regular institutional dialogue under the auspices of the UN. *Session reports from the event will be available on the Digital Watch observatory.*

9–27 SEPTEMBER
42nd Session of the Human Rights Council (Geneva)
The 42nd session of the Human Rights Council will feature high-level discussions on human-rights-related issues, such as the right to privacy, the rights of persons with disabilities, the rights of minorities, and the rights of children. *Session reports from the event will be available on the Digital Watch observatory.*

17–30 SEPTEMBER
74th Session of the UN General Assembly (New York)

'Galvanising multilateral efforts for poverty eradication, quality education, climate action, and inclusion' is the theme of the 74th Session of the UN General Assembly (UNGA). Peace and security is also a priority area that member states are encouraged to focus on. World leaders are expected to deliver statements outlining existing and future plans for multilateral initiatives that ensure sustainable development. *An analysis of the digital issues covered by the speeches will be available on the Digital Watch observatory.*

18 SEPTEMBER
Digital (and) Diplomacy: How to deal with digital aspects of foreign policy (Geneva)

Organised by DiploFoundation, the conference will address emerging models of digital and tech diplomacy, the interaction of countries with the tech industry and innovation hubs, and how digital diplomacy in Geneva should cover complex digital policy processes. Key challenges for diplomatic practice in the digital age will also be discussed, including how small and developing countries keep up with digital policy developments, the impact of big data and AI on diplomacy, and the skills and knowledge needed for digital diplomacy. The conference contributes to the implementation of the recommendations of the UN High-Level Panel on Digital Cooperation, which identified lack of diplomatic capacities as one of the challenges for digital co-operation.

26–28 SEPTEMBER
The Common Good in the Digital Age (Vatican)

Organised by the Dicastery for Promoting Integral Human Development and the Pontifical Council for Culture, the seminar will promote an in-depth discussion on the common good in the digital era. The three-day event will feature debates on a wide range of topics, including peace and warfare in the digital age, the future of work, and ethical dilemmas associated with developments in AI, blockchain, and automation. Participants will include experts from different backgrounds, including science, technology, government and regulation, economics, social sciences, and theology.

October

# Test your knowledge on national AI strategies

As AI technologies continue to evolve, countries are increasingly developing national AI plans and strategies to help them take advantage of AI progress. Are such strategies in force or in the making? And what do they focus on? Test your knowledge with our crossword. Articles in this issue, and our dedicated AI space on the *Digital Watch* observatory, can help you find the answers.

Across

1 In February 2019, US President Donald Trump signed an executive order dedicated to maintaining American _____ in AI. (10)

4 Not only countries are developing their strategies; regions are doing so too. One example is the AI plan developed in early 2019 by the _____ region in Belgium. (7)

9 AI _____ and development (also known as R&D) is a key area in multiple national AI strategies, as it aims to direct considerable financial resources in this direction. (8)

10 In the USA, the Department of _____ launched an AI strategy to accelerate the adoption of AI in military decision-making and operations. (7)

13 Incoming President of the European _____, Ursula von der Leyen, announced that AI will be among her top priorities for the next five years. (10)

14 France's AI strategy is based on a comprehensive report prepared by French mathematician and politician Cedric _____. (7)

Down

2 Since data is crucial for the development of AI applications, many national AI plans say that public authorities need to make their ____ ____ available for reuse by other stakeholders. (two words) (4,4)

3 Due to AI's potential implications for human rights, some strategies call for _____ frameworks to guide the development and use of AI applications. (7)

5 According to reports, although the European Commission recommended that EU countries have national AI plans in place by mid-2019, there are _____ member states which have not yet reached this milestone. (5)

6 This type of co-operation among countries is needed, according to several national AI plans and strategies. (13)

7 A recent report from the US National Institute of Standards and Technology encourages the US federal government to get more engaged in the development of AI technical _____. (9)

8 As AI is bringing many changes to the world of work, governments will need to focused on preparing the country's_____ for such changes. (9)

11 The United Arab Emirates has appointed a State _____ for AI, to oversee the implementation of the country's AI strategy. (8)

12 One of the objectives of the Czech national AI strategy is to develop national _____ of excellence in AI. (7)

13 In 2017, this country released an ambitious national AI development plan which promises to transform it into the world leader in AI by 2020. (5)
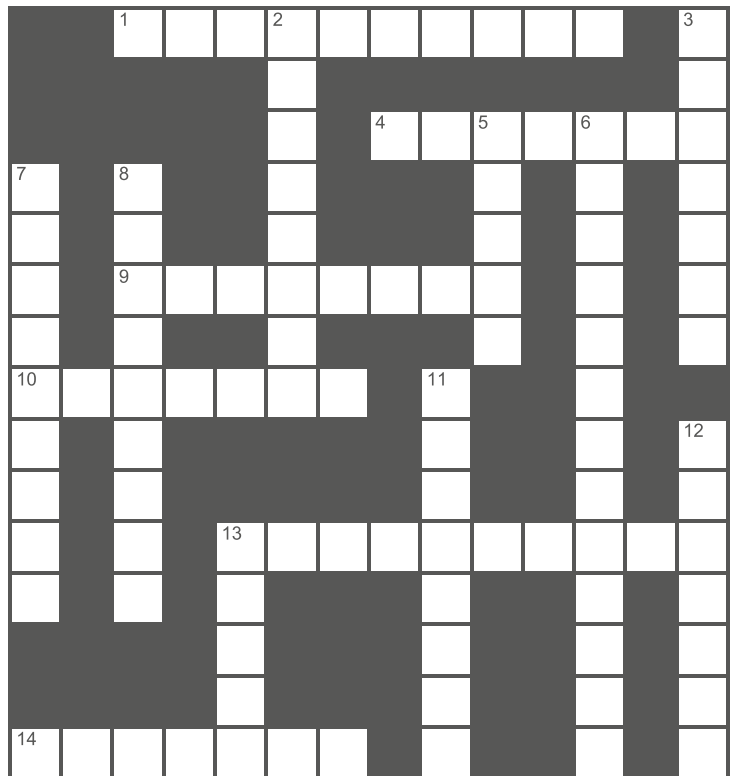
Across: 1 Leadership, **4** Flemish, **9** Research, **10** Defense, **13** Commission, **14** Villani.
Down: 2 Data sets, **3** Ethical, **5** Eight, **6** International, **7** Standards, **8** Workforce, **11** Minister, **12** Centres, **13** China.

Geneva Internet Platform
DigitalWatch

The Geneva Internet Platform is an initiative of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

RÉPUBLIQUE ET CANTON DE GENÈVE

UNIVERSITÉ DE GENÈVE

ETH zürich

DiPLO
www.diplomacy.edu