# Top digital policy developments in 2017

## A year in review

Geneva Internet Platform

DigitalWatch

# Top digital policy developments in 2017
## A year in review

IMPRESSUM



Published by the Geneva Internet Platform and DiploFoundation (January, 2018)

Download the digital version from https://dig.watch/2017

The digital version contains links to additional resources. Click on the resource icon to access more details. Click on the observatory icons to learn more about each issue.

WMO Building (2nd floor)
7bis, Avenue de la Paix
CH-1202 Geneva, Switzerland
E-mail: gip@diplomacy.edu

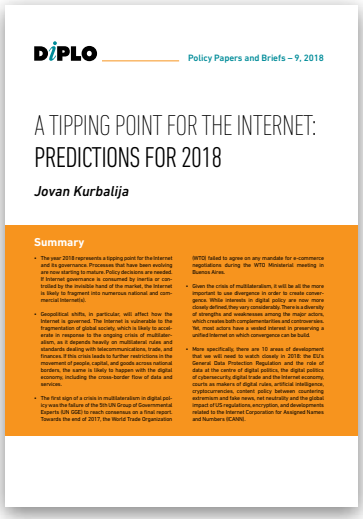
**Contributors:** Stephanie Borg Psaila, Arvin Kamberi, Jovan Kurbalija, Marilia Maciel, Virginia Paque, Roxana Radu, Vladimir Radunovic, Barbara Rosen Jacobson, Sorina Teleanu

**Copy-editing:** Mary Murphy

**Design and layout:** Viktor Mijatović, Mina Mudrić, Aleksandar Nedeljkov

**A tipping point for the Internet: 10 predictions for 2018**

Complement your overview of digital policy with an analysis of what to expect in 2018. In his predictions, Dr Jovan Kurbalija looks at 10 key areas, including data and digital politics, cybersecurity, artificial intelligence, and digital trade, and argues that the year will be crucial for making policy decisions with longer-term impact. 'If Internet governance is consumed by inertia or controlled by the invisible hand of the market, the Internet is likely to fragment into numerous national and commercial Internet(s).' Download the briefing paper or read the online article.


DiPLO Policy Papers and Briefs – 9, 2018

A TIPPING POINT FOR THE INTERNET: PREDICTIONS FOR 2018

*Jovan Kurbalija*

Summary

# Overview

Continuing an exercise we started in 2017, we look back at the top developments that shaped digital policy in the year that has just ended. Some developments were on a constant high throughout the year, such as those related to cybersecurity and digital rights. The fight against violent extremism and fake news increased in prominence during 2017.

The year saw new technologies – such as artificial intelligence (AI) and cryptocurrency – picking up pace. AI triggered concerns over lethal autonomous weapon systems (LAWS) and a race for supremacy among ambitious states.

The private sector faced increasing demands by governments: Internet platforms were asked to remove illegal content more swiftly; companies faced more pressure to 'pay their fair share' of taxes. The industry also played a prominent role in proposing cyber-norms.

Digitisation raised issues on the future of work, while some of the questions related to the sharing economy were answered by courts, which continued to shape digital policy through numerous rulings.

This report sums up the top 20 digital policy developments for 2017 (in thematic sequence), and is based on developments which expert curators from the Geneva Internet Platform analysed every month for the *GIP Digital Watch* observatory.

Our reflections will continue throughout 2018. Join our briefings on the last Tuesday of every month for a regular recap of global and regional developments. The developments are further analysed in the monthly newsletter, available in English, French, Spanish, and Bahasa Indonesian (with more languages planned for 2018); download the newsletter on the last day of each month.

Find all the latest updates, trends, processes, and other resources on the *Digital Watch* observatory at https://dig.watch, and keep track of global events using DeadlineR, our notification system accessible through our calendar of digital policy events.

*Comments are welcome. Get in touch via gip@diplomacy.edu*

**The main developments in 2017:**

# #1 Private sector proposes cyber-norms

One of the main developments in 2017 was the private sector's proposals of cyber-norms to protect cyberspace. In February 2017, Microsoft's President and CLO Brad Smith proposed a Digital Geneva Convention, which should 'commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure.' The proposed convention, which attracted the attention of the global digital policy community, should also motivate states to adhere to agreed norms, which have emerged in recent years, and adopt new and binding rules.

Among the 10 key clauses proposed by Microsoft are the need for states to refrain from attacking systems that are important for the safety and security of citizens or the global economy, and the need to limit engagement in cyber-offensive operations that could damage such infrastructures. Other clauses touch on the issue of privacy, as well as the theft of intellectual property.

In April 2017, Smith announced three new documents that continue to shape the company's proposal: the first carries key clauses which should form part of the convention; the second outlines a common set of principles and behaviours for the tech sector to help protect civilians in cyberspace; the third proposes the setting up of an independent attribution organisation to identify wrongdoing.

In November, as he recalled the origins of the International Committee of the Red Cross, and the experiences of Henri Dunant in the aftermath of the Battle of Solferino which inspired its creation, Smith reiterated the call at the Palais des Nations in Geneva.

Google also made a proposal of its own: In June, it published a proposal that would allow law enforcement to request digital evidence directly from Internet companies, bypassing the need to go through slow, cumbersome channels, such as the Mutual Legal Assistance Treaties (MLATs) framework.

According to Google's proposal, this would work only with countries that adhere to privacy, human rights, and due process standards.

## Why is this significant?

With these two proposals, the industry showed that it was increasingly stepping into a norm-developing role, which previously had been mainly the ambit of governments.

Warfare in cyberspace involves infrastructure that is operated by private companies such as Microsoft. Warfare therefore carries a huge cost for the industry, and in the case of larger infrastructures, the cost is larger.

It is, therefore, in the company's interest for governments and industry to agree on norms that will protect cyberspace.

Similarly, the Internet industry was under increasing pressure by governments to provide digital information – as we saw in 2016 in the Apple/FBI saga – to be used in criminal investigations and anti-terrorist activities. The industry was ready to find alternatives to dealing with a patchwork of legislation.

### Surveillance treaty in the making

In parallel with the proposed cyber norms, the UN Special Rapporteur on privacy proposed a surveillance treaty in his 2017 report to the Human Rights Council.

Aiming to address surveillance activities for national security purposes that fall beyond the scope of existing international instruments, the treaty would co-exist alongside other instruments – such as the Cybercrime Convention. According to the Special Rapporteur, the lack of regulation of this type of surveillance poses high risks for privacy protection. The treaty is expected to be tabled in early 2018.

FOLLOW THE ISSUES

Cybersecurity | Intermediaries | Jurisdiction

# #2 UN GGE ends without consensus

The fifth UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) ended without consensus. In the weeks that followed, a debate picked up on the future of the UN GGE, and potential solutions for a global cybersecurity forum. The UN GGE, tasked to examine cyberthreats and make recommendations, was unable to reach consensus over its final report during its last meeting on 19–23 June 2017. The report of the UN-mandated group – which was being reconstituted every two years – represents the main outcome of its work.

## Why is this significant?

Previous reports introduced the principle that existing international law applies to the digital space, and developed voluntary norms and principles of responsible behaviour of states in cyberspace – both of which are considered to be major achievements. Although the reports are not legally binding, they carry significant influence in the field of global cybersecurity.

The UN GGE's future is uncertain: in the aftermath, some states suggested an open-ended working group, while others said that different options should be considered. In its absence, bilateral agreements – predominant in the past few years – continue to be adopted, in addition to regional and subregional agreements, such as in the Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and Association of Southeast Asian Nations (ASEAN). But the search for a global mechanism continues.

### What could a global cybersecurity mechanism look like?

In January 2018, Dr Jovan Kurbalija, Head of the Geneva Internet Platform, predicted that the search for cybersecurity solutions will intensify, and listed potential solutions for a global mechanism:

**A continuation of the UN GGE process:** Although there is little appetite for more of the same, a sixth UN GGE could take up Russia's proposal for a Code of Conduct, or could operationalise the 2015 UN GGE report.

**A UN Open-ended Working Group on ICT Security,** proposed by the Group of 77 in the framework of the UN General Assembly (UNGA), could develop actionable recommendations including a proposal for drafting a cybersecurity treaty.

**A UN Conference on Disarmament**: Although it is formally possible to include cybersecurity in the activities of the UN Conference on Disarmament, this is unlikely to be a viable option unless it overcomes inclusivity and transparency concerns.

**International Telecommunication Regulations (ITRs)** could include emerging cybersecurity issues; this is a new turn, following a recent Chinese proposal for a meeting of the Expert Group on ITRs at the International Telecommunication Union.

**A Committee on the Peaceful Uses of ICT (COPUICT)** could anchor digital discussion in the UN functional trinity: peace, security, and development. Analogous to outer space, COPUICT could focus on scientific, technical, and legal issues.

**Regional cooperation:** In 2018, regional organisations could play an important role in implementing recommendations made by the 2015 UN GGE Report, particularly through different confidence-building measures, and the implementation of the non-controversial parts of the last UN GGE deliberations, such as those on capacity development.

**Private sector initiatives:** Since the business sector is most vulnerable to cybersecurity risks, business initiatives will accelerate, giving priority to technical attribution of cyber-attacks.

*In more detail: Kurbalija J (2018) A tipping point for the Internet: 10 predictions for 2018. DiploFoundation Policy Papers and Briefs, No. 9*


FOLLOW THE ISSUES

Cybercrime | Cybersecurity | Cyberconflict | Critical infrastructure

# #3 WannaCry becomes the biggest ransomware in history

On 12 May 2017, new ransomware WannaCry attacked a Spanish mobile operator, followed by hospitals and clinics across the UK. Within hours, the malicious software spread across almost 100 countries, including Russia and the USA. It was said to be the biggest ransomware outbreak of all times.

Ransomware is performed by a type of malicious software that blocks access to a computer system or data, usually by encrypting it, and demands a payment to release the files. Like other malicious software, WannaCry encrypted data on the device and demanded a ransom of USD$300 to be paid to a given bitcoin wallet within three days.

Unlike other viruses, however, WannaCry propagated through the network and infected computers like a worm, which meant that their users did not have to activate the infected file or link for the software to continue spreading. The ransomware was stopped accidentally by a researcher.

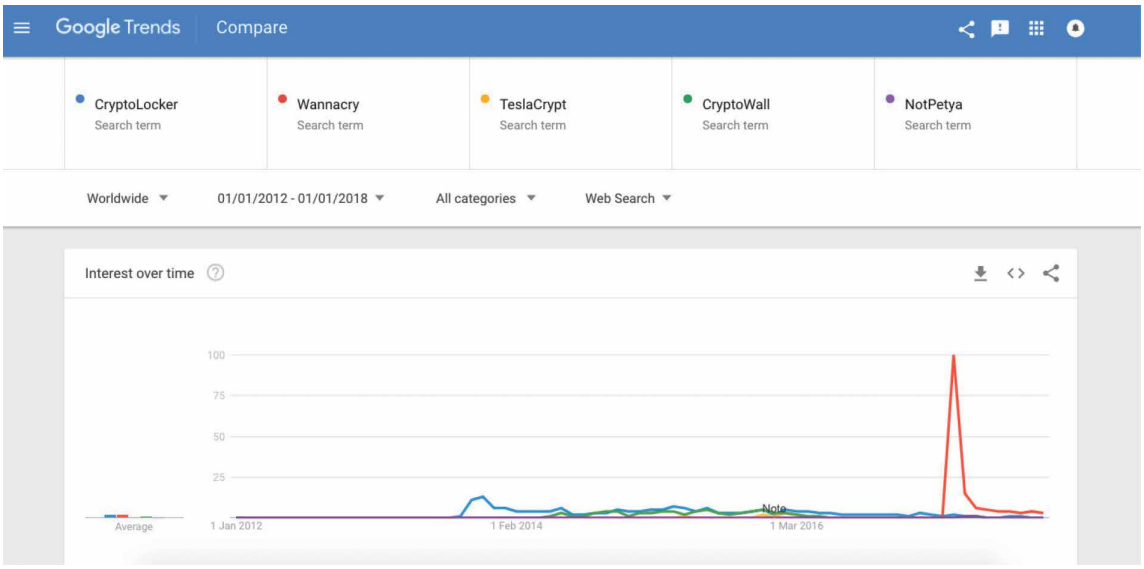
## Why is this significant?

In recent years, there has been a shift in ransomware targets. In search for larger financial gains, perpetrators have turned from individuals to businesses. The services sector is reportedly the most affected sector. Business targets are often small to medium-sized organisations with immature IT infrastructures and a limited ability to recover from such an attack. The attacks in 2017 show that organisations controlling sensitive data, such as the healthcare industry in particular, have been increasingly affected.

The losses suffered from these malware attacks are usually significant. In addition to the ransom itself (which arguably did not raise large sums), the attacks created a significant disruption to the hospital system in the UK, and to other critical infrastructure around the world. As the WannaCry attack showed, ransomware can disrupt digital commerce and society overall, either in direct or indirect ways. Other negative losses can include temporary or permanent loss of sensitive or proprietary information, financial losses incurred to restore the systems and files, and potential harm to reputation.

Beyond the losses it generated, the attack received widespread media attention. For the first time in history, the attack brought cyberattacks and ransomware to the public's attention. Google's search trends for the past five years show that WannaCry was the most searched for term from among other major ransomware software. The attack also led Microsoft's President and Chief Legal Officer, Brad Smith to reiterate a stronger call for the Digital Geneva Convention, first proposed in February 2017.

*View the interactive map of the countries that were hit by the WannaCry ransomware, and learn how it happened and what the response was.*




**FOLLOW THE ISSUES**

Cybercrime | Cybersecurity | Telecommunications infrastructure | E-Money and virtual currencies

# #4 Data breaches and vulnerabilities raise disclosure issue

The number of data breaches in 2017 is substantial, and show that user data is far from safe. Users learn about a data breach only after it is revealed by the companies. In Uber's case, news of a breach that affected the data of 57 million drivers was disclosed a year later, in November 2017. At this time, it also emerged that after the company's servers were breached in 2016, Uber paid $100,000 to the intruders to delete the data and keep silent.

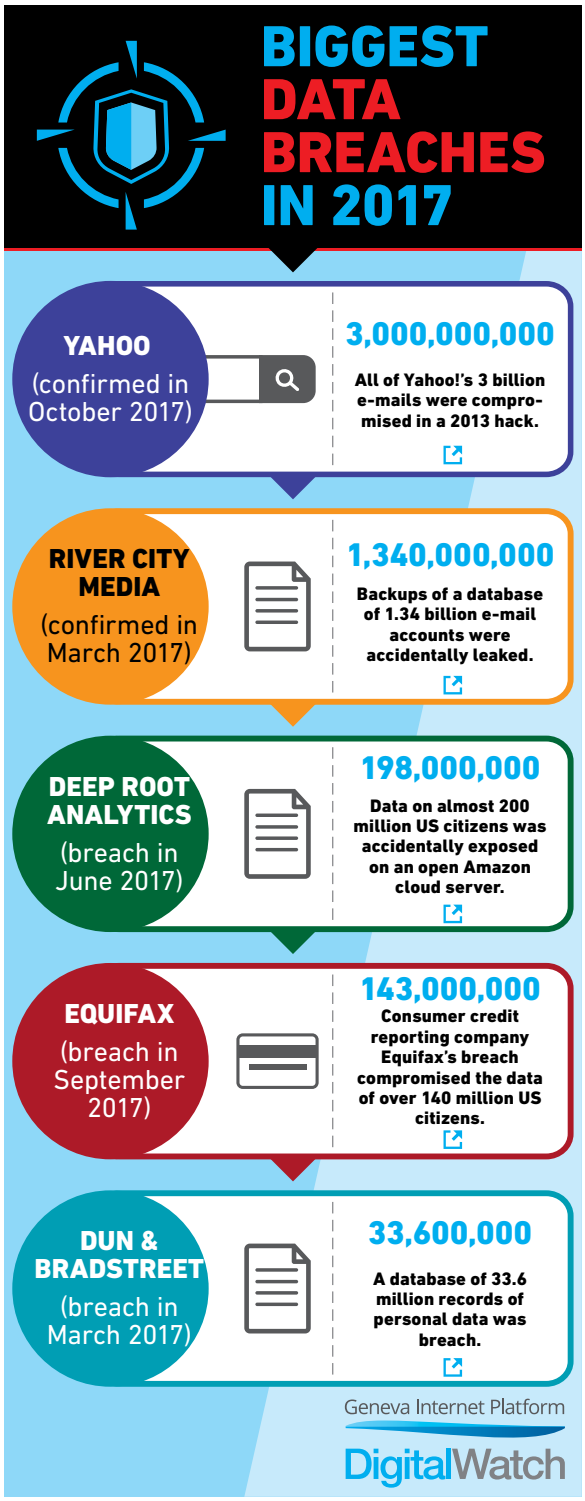
Hacks are also on the increase, and the issue is closely related to vulnerabilities discovered by governments. In March 2017, WikiLeaks released over 8000 pages of confidential US government documents, dating from 2013 to 2016, that provided a detailed description of the CIA's ability to hack phones, computers, and smart devices. The leaks, known as Vault 7, revealed that the CIA is able to compromise the software of all the major technology vendors.

In November 2017, the US White House released an updated version of its Vulnerability Equity Process (VEP), according to which US security agencies decide which of the vulnerabilities they have discovered will be disclosed to the software's developer, and which will be withheld. The White House Cybersecurity Coordinator revealed that the US government discloses more than 90% of the vulnerabilities it finds.

## Why is this significant?

Legal frameworks around the world oblige companies to disclose their breaches. Even though the companies can suffer reputational damage and financial losses, users have a right to know. If credentials are stolen, they need to update their log-in details; if financial data is stolen, they may need to talk to their banks. The questions are: How promptly should breaches be disclosed, and is there any liability?

When it comes to vulnerabilities, there are no obligations to report on vulnerabilities discovered, nor are software and hardware vendors liable for the insecurity of their products. Non-disclosed vulnerabilities can cause havoc if they are leaked, as the WannaCry ransomware showed. As whistleblower Edward Snowden warned, the nondisclosure of 10 significant security flaws outweighs the benefits of disclosing 90 low-severity flaws.



# #5 Governments strengthen demands for swift removal of extremist content

Extremist content has been plaguing the Internet in the past few years. The industry has responded by creating new initiatives and measures – such as the Global Internet Forum to Counter Terrorism – to combat the spread and to speed up its removal. Despite the measures, pressure from governments continued in 2017.

The fight against extremist content was one of the top issues during the 72nd UNGA debate. UK Prime Minister Theresa May called on tech companies to act. The EU called on the major online companies to develop the means for automatic deletion of extremist content immediately after posting. At a dedicated discussion in a parallel event to the UNGA meeting, May called on Internet companies to remove extremist content within one to two hours of posting. The industry indicated that the increased efforts would be 'an enormous technological and scientific challenge'. Yet, governments will not turn a blind eye.

In Germany, a new law which was passed in 2017 and entered into force on 1 January 2018, requires Internet platforms with more than two million users to proactively report and delete illegal content. Content needs to be removed within 24 hours after receiving a complaint in obvious cases, and within one week in more complex situations. If these deadlines are not observed, companies will face fines of up to €50 million. Companies have said the law may pose a challenge, considering the hundreds of thousands of complaints they receive every week; and other critics fear that the law could lead to reduced Internet freedom, as companies might remove more content than necessary to avoid fines.

## Why is this significant?

The war against extremist content has placed Internet companies at the front line. As de facto gate-keepers of Internet content, they are under pressure to police the content, and remove the illegal content swiftly. Many governments, however, remain unconvinced, claiming that companies are not sufficiently proactive. At the end of 2017, the UK government made it clear that if it was forced to act, the industry would be faced with taxes to set off the large cost of de-radicalisation. This trend is likely to continue in 2018, with other countries also opting for increased regulation and penalties for lack of sufficient action.

To counter extremist content, companies used to rely on content moderators to review and remove inappropriate content. Yet it became increasingly clear in 2017 that these measures are unsustainable due to the risk of psychological harm to the moderators, and their incapacity to properly monitor all problematic content on the platforms. Companies therefore started employing other measures, including AI tools. An unwanted by-product was the erroneous removal of legitimate content. The false-positives included content used or uploaded by journalists, investigators, and organisations reporting on conflict zones and human rights crises – content which serves as historical record, and which could be used in legal proceedings.

**Spotlight: The Global Internet Forum to Counter Terrorism**

Launched in July 2017, the forum focuses on:

1. **Employing the technology to find solutions:** By December 2017, the shared industry hash database – which allows the industry to identify content through digital fingerprints (or hashes) – had over 40,000 pieces of content.
2. **Research:** The forum will commission and fund research to inform efforts and to guide policy decisions.
3. **Knowledge-sharing:** The forum is engaging with small companies to share best practices on how to disrupt the spread of violent extremist material. This is being done through the Tech Against Terrorism initiative in partnership with ICT4Peace and the UN Counter Terrorism Executive Directorate. Participation at high-level events and holding workshops for companies complement this goal.

*Learn more: Update on the Global Internet Forum to Counter Terrorism*


**FOLLOW THE ISSUES**

Content policy | Intermediaries | Jurisdiction

# #6 Intermediaries battle spread of fake news

What started as a major concern in the USA after the 2016 Presidential election became a global concern for authorities, the industry, and users. Chosen as the word of the year 2017 by the Collins Dictionary, fake news gave rise to a wide range of questions, from semantic (whether fake news is an accurate term or others – like misinformation or information disorder – are more appropriate) to philosophical (truth in the modern era), and from operational (attribution of fake news) to the implications for the democratic process (use of fake news for political aims).

Much of the public debate focused on the responsibility of Internet intermediaries in dealing with the content they host. Faced with increasing pressure from governments, Internet companies started taking more measures to tackle fake news.

In February 2017, Facebook announced that it was starting to test fake news filtering tools in Germany. In France, Facebook and Google partnered with news organisations to launch new fact-checking tools to minimise the risks of fake news affecting the presidential election. Google added a fact-checking feature to Google Search and Google News, presenting information from fact-checking organisations in search and news results worldwide. Facebook announced new moves to help suppress fake news in advance of the general elections in the UK, including deleting thousands of fake profiles, and working together with a fact-checking charity.

## Why is this significant?

Fake news can lead to massive misinformation and have adverse political consequences, so there is a general agreement that action is needed to address such risks. But is it the right answer to place increased responsibility on Internet intermediaries? If they become more active in filtering and suppressing content that could contain fake information, isn't there a risk of infringing freedom of expression? And is it even realistic to expect intermediaries to be able to filter through the millions of posts that are published on their platforms every day? If this is a task entrusted to AI and automatic filters, can technology be fully trusted not to make biased decisions?

In light of these and similar questions, fact-checking initiatives seem to become more and more widespread, and Internet companies partner with media and fact-checking organisations in this regard. But is this enough? Many argue that there should be more focus on awareness-raising and education, especially when it comes to developing the critical thinking of Internet users, and their ability to validate information.

**European Commission's initiative: Expert group and public consultations**

In November, the European Commission announced the setting-up of a High-Level Expert Group on fake news and online disinformation, with representatives of academia, the tech industry, news media, and civil society. The group will advise the Commission 'on scoping the phenomenon of fake news, defining the roles and responsibilities of relevant stakeholders, grasping the international dimension, taking stock of the positions at stake, and formulating recommendations'.

The Commission, which plans to present its strategy on countering fake news in the spring of 2018, also launched a public consultation to collect information on how to define fake news and their online disinformation, measures taken to counter the spread of fake information, and future action to strengthen quality information and prevent the spread of disinformation. The consultation runs until 28 February 2017.


FOLLOW THE ISSUES

Intermediaries | Content policy | Jurisdiction

# #7 Concern over LAWS as the debate picks up

If AI pioneers warn about AI risks, the world stops to listen. In 2017, over 100 AI experts warned against the development of lethal autonomous weapons, or the so-called killer robots.

The signatories' call on the Group of Governmental Experts (GGE) on Lethal Autonomous Weapon Systems (LAWS) to find solutions to this growing problem came a few months before the group met in November 2017 for the first time. The GGE was established by the High Contracting Parties to the Convention on Certain Conventional Weapons (CCW) to explore the technical, military, legal, and ethical implications of LAWS.

## Why is this significant?

Echoing a first warning they made in 2015, Tesla CEO Elon Musk and Deep Mind Head of Applied AI Mustafa Suleyman were among those who warned the UN that 'lethal autonomous weapons threaten to become the third revolution in warfare'.

'Once developed', the pioneers wrote, 'they will permit armed conflicts to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways.'

Convening in Geneva, the GGE concluded that policy options could include a legal instrument, such as an additional protocol, prohibiting LAWS, or a politically binding declaration, or a future Code of Conduct. A moratorium was also suggested, with the caveat that it would be premature if such weapons have not yet been developed.

The next GGE meetings take place in April and August 2018.

**The first GGE meeting: Mapping the debate**

Although the debate on LAWS is not new, the GGE tackled the issues systematically. The following are the main debates and conclusions:

- Despite the establishment of a GGE on LAWS, there is no clear agreement on a definition of LAWS. To what extent are these weapons autonomous, and what is the necessary level of meaningful human control?
- The challenges range from technological and military, to legal and ethical, including their potential unreliability, their proliferation, their legal accountability, and the absence of human decisions on life and death.
- The issues are complex since the technologies driving AI and robotics can be used for both civilian and military purposes. There is a concern that restrictions on LAWS could hamper innovation for the civilian use of these technologies. At the same time, technologies designed for civilian use might be transformed into lethal weapons.
- LAWS need to comply with international humanitarian law and human rights law. Their development is already scrutinised under the Additional Protocol I to the Geneva Conventions although the existing provisions are arguably insufficient.
- States have a responsibility during the deployment of LAWS in armed conflict. Potential military applications need to be kept under review.

*In more detail: Rosen Jacobson B (2017) Lethal Autonomous Weapons Systems: mapping the GGE Debate. DiploFoundation Policy Papers and Briefs, No. 8.*


FOLLOW THE ISSUES

Convergence | Cyberconflict

# #8 Race for AI supremacy intensifies

'Whoever becomes the leader in this sphere will become the ruler of the world', Russian president Vladimir Putin warned, while speaking about his country's efforts to achieve excellence in AI.

Russia is not the only country that has started to place AI at the core of its development strategies. Governments have become more aware of AI's potential, and have started elaborating strategic plans to position them at the forefront of developments.

China announced a Next Generation Artificial Intelligence Development Plan to transform the country into 'the world's primary AI innovation centre' by 2030. The United Arab Emirates released an AI strategy and appointed a State Minister for Artificial Intelligence. In the UK, a report commissioned by the government recommended a series of actions to transform the UK into 'the best place in the world for business developing and deploying AI to start, grow, and thrive'. These are only some examples.

## Why is this significant?

AI comes with numerous opportunities, but also with challenges and risks. As Stephen Hawking says, it could be 'the best or the worst thing ever to happen to humanity'. The opportunities are obvious, if we look at AI applications in areas such as smart buildings, medical robots, translation tools, and intelligent education systems.

AI can also lead to economic growth and sustainable development, and has an enormous potential to bring positive change in society. So, it is encouraging news that governments are stepping in to support AI progress.

But there are also concerns over possible unintended consequences and the impact on the economic, social, and cultural aspects of society. Many concerns are related to the disruptions that AI systems could bring on the labour market, as automated systems are likely to make some jobs obsolete.

There are worries about safety and security (such as in the context of self-driving cars); about privacy and data protection (given the enormous amounts of data that AI systems work with); and about ethics, accountability, and transparency. While governments look into supporting advancements in AI, can they also find solutions to these and other challenges? And is this only their responsibility, or should other stakeholders have a role to play as well?

**Initiatives tackling AI challenges**

The year 2017 saw more stakeholders considering the challenges that come with AI technological developments. In the UK, the House of Lords created a Select Committee on Artificial Intelligence, to explore the economic, ethical, and social implications of AI. Germany and the USA adopted ethics and safety guidelines to be considered in the development of automated driving systems. Estonia started considering legislation to address the legal status of AI systems.

The Information Technology Industry Council, representing companies such as Apple, Amazon, Facebook, Google, and Microsoft, adopted a set of Policy principles aimed at guiding 'industry and governments to ensure AI's responsible growth and deployment'. DeepMind created an Ethics & Society research unit to explore real-world impacts of AI and key ethical challenges. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems published the second version of its Ethically Aligned Design document, looking at how we can integrate values and ethical principles into the design of autonomous systems.


FOLLOW THE ISSUES

Convergence | Cyberconflict

# #9 Debating the future of work

Jobs and employment were high on the digital agenda in 2017. While there seemed to be broad agreement on the fact that digitalisation, automation, and AI will bring transformations on the jobs market, there were different views on how disruptive these transformations will be.

A report published by McKinsey in January 2017 noted that the impact of automation on workers will vary across different activities, occupations, and wage and skills levels. Less than 5% of occupations are candidates for full automation, but almost every occupation has partial automation potential. When it comes to individual work activities, half of them (in the form they have today) could be automated by 2055.

In October 2017, a PricewaterhouseCoopers report predicted that 30% of jobs in Organisation for Economic Co-operation and Development (OECD) countries would be at risk of automation. But the risk of automation varies considerably across industries, with transport, manufacturing, and retail facing some of the largest risks, while health and social work, arts and entertainment, and education face the lowest risks.

At the end of the year, McKinsey predicted that between 400 and 800 million individuals could be displaced by automation and would need to find new jobs by 2030. New jobs will be available, but people will need to be retrained and learn new skills, as many of them will need to switch occupational categories.

Millennials tend to be optimistic: According to a survey conducted by the World Economic Forum, they believe that technologies, including AI and robotics, are creating jobs more than destroying them.

## Why is this significant?

There are different predictions as to how the world of work will be impacted by new technologies. Some are optimistic: Just as the workforce adapted during previous industrial revolutions, it will also be able to adapt in this case. Others are more concerned: There will be significant occupational changes, job polarisation, and gaps in social protection.

In all these debates, many turn to governments, asking them to make sure that, as digital progress continues to shape our societies, no one is left behind, and people are placed at the core of digital policies. How exactly these policies should be shaped remains a matter for discussion.

Some are asking for changes to current labour and employment legislation to make them better suited to the protection of workers' rights.

Others are calling for universal basic incomes to compensate individuals for disruptions in the labour market as a result of automated systems.

One point of convergence refers to the need for education and training systems to be adapted to the new requirements of the jobs market, and for the current workforce and new generations to be prepared to respond to these requirements.

**In focus: The Future of Work Initiative**

In preparation for its 2019 centennial anniversary, the International Labour Organization (ILO) launched the Future of Work Initiative, to identify ways in which the ILO can respond to the challenges posed by the changes in the world of work.

- In April, *The future of work we want: A global dialogue* conference concluded, among others, that 'the future of work must be inspired by considerations of humanity, social justice, and peace.'
- In August, a high-level Global Commission on the Future of Work was created. It will develop a report on 'how to achieve a future of work that provides decent and sustainable opportunities for all.'
- In December, an Inception Report set the scene for the work of the Commission. It draws attention, among others, to the need for educational institutions to focus less on training technical skills and more on developing competences, such as cognitive and problem-solving abilities.

**FOLLOW THE ISSUES**

**Labour law**

**Other economic issues**

# #10 Courts continue to shape digital policy

It has been predicted that 'in the search for solutions to their digital problems, Internet users and organisations will increasingly refer to courts. Judges could become de facto rule-makers in the field of digital policy'.

In previous years, court judgments created tectonic shifts in certain policy areas. Among them were the Max Schrems ruling which invalidated the Safe Harbour Agreement, and led to the creation of the new Privacy Shield, offering privacy safeguards to data transfers of European citizens to the USA. The Mario Costeja González ruling recognised users' right to be forgotten, and led tens of thousands of users to request search engines to delist them from search results.

In 2017, court rulings show that predictions for the year were accurate. The Court of Justice of the European Union (CJEU) issued the much-awaited decision that Uber is a transportation company, and not a provider of information society services. In the USA, a court dismissed two lawsuits that accused Facebook of supporting terrorist groups by allowing them to use the platform for the pursuit of terrorist goals.

In Germany, a regional court judged that Facebook users are not liable for unlawful content if they only share it. In India, the Supreme Court ruled that the right to privacy is a fundamental right, overruling an earlier lower court judgment declaring the contrary.

## Why is this significant?

Courts increasingly tend to fill in the void created by the lack of clear digital policies in certain areas. Rulings that delineate the responsibility of Internet intermediaries are one example. The question is whether it is desirable, in the long term, for courts to step into the shoes of legislative bodies.

At the same time, court judgements shape the applicability of digital policy both within and beyond national jurisdictions. Several rulings – most notably related to the right to be delisted – have extended their reach, drawing criticism over the risk of breaching users' freedom of speech and freedom of press in other parts of the world.

In addition, cross-border rulings add new challenges to an already-complex digital space, as they can give rise to conflicting rulings. Such was the case concerning the right to be forgotten in Canada: In June 2017, the Canadian Supreme Court ordered Google to remove search results that violated intellectual property rights worldwide; in October 2017, a US judge blocked the decision being applicable in the USA.

In deciding on issues that have cross-border implications, courts will need to assess the widest possible implications.

**Long-arm jurisdiction: The main cross-border cases in 2017**

In recent years, the right to be forgotten (or delisted) has continued to be shaped by courts worldwide. The battle between Google and the French data protection regulator (the *Commission nationale de l'informatique et des libertés – CNIL*) escalated after Google appealed the regulator's decision to fine the company for not delisting across all of its websites. In July 2017, the French supreme administrative court passed the matter to the CJEU.

The Canadian Supreme Court's June 2017 ruling was blocked in the USA, at Google's request, which brought the company both a win and a challenge: Can Google choose not to abide by a cross-border ruling issued by Canada's court, and will that be tantamount to contempt of court?

Social media networks have also been affected by cross-border rulings. In May, an Austrian court ordered Facebook to remove posts reflecting hate speech not only in Austria, but across the platform. In Australia, Twitter was ordered to prevent a particular user from opening an account anywhere in the world.

**FOLLOW THE ISSUES**

Jurisdiction | Intermediaries | Consumer protection

# #11 National governments join in regulatory race

IIn addition to courts, national governments also started filling the regulatory gap by adopting a wide range of national laws whose impact goes beyond their borders.

For many years, the USA was considered one of the countries which strongly supported the principles of net neutrality; the Open Internet Order was proclaimed a success by net neutrality activists around the world. The repeal of the order was considered a blow for net neutrality. The effects go beyond the criticism it attracted from users and companies in the USA. It can now influence how other countries regulate this area. *More: #15 Net neutrality dealt a blow*

China's cybersecurity law, which came into effect on 1 June 2017, imposed restrictions on the transfer of data overseas: personal data of Chinese users must be stored domestically. Russia has similar legislation: User data needs to be stored on local servers.

The EU's General Data Protection Regulation (GDPR), albeit passed at regional level, also extends its reach beyond European borders. *More: #13 Industry prepares for GDPR*

## Why is this significant?

Countries often have different priorities, needs, and values. What is deemed important in one country may not be the case in another. To achieve their aims, countries address policy gaps through local legislation. The Internet, however, follows a different logic as it is, by its nature, borderless.

This lack of a harmonised approach can result in a patchwork of national legislation that can create conflicts across jurisdictions, and cause uncertainty for businesses. Conflicting laws can impact e-commerce, privacy, and content policy, among others.

The impact can range from influencing other countries' policies, to affecting data flows and the movement of goods and services. The US Federal Communications Commission (FCC) decision to reverse the Open Internet Order may influence how other countries tackle the issue. Weakened rules in one country, for example, could motivate other countries to adopt stronger protection for net neutrality principles. Localisation rules have a more direct effect. Since data is considered the world's most valuable resource, countries use the rules to attract investment and exert influence over Internet companies.

**AI and IoT: Regulation is needed, stakeholders reiterate**

Two areas in which stakeholders felt that regulation was needed were the Internet of Things (IoT) and artificial intelligence sectors.

As IoT devices become more prevalent in our lives, they remain highly vulnerable to cyber-attacks. In February, IBM called for the creation of a new government agency in the USA to regulate the sector and ensure security standards. The company's Chief Technology Officer pointed out that cybersecurity risks associated with IoT require governmental intervention, as 'the market is not going to fix this, because neither the buyer nor the seller cares'. In a paper issued in May 2017, Microsoft took a more cautionary approach, noting that governments can be catalysts for good IoT security practices.

Concerns surrounding the impact of AI on society at large also led to calls for governmental regulation. In April 2017, the International Bar Association Global Employment Institute noted that 'governments have to become more active' and adapt current labour and employment legislation to an emerging workplace reality where changes are driven by automation and AI. In June, researchers from the Alan Turing Institute argued that 'precise regulation' is needed to create fair and accountable AI and robotics.


FOLLOW THE ISSUES

Jurisdiction | Privacy and data protection | Net neutrality | Other economic issues

# #12 Uber confirmed a transport company; effects on the sharing economy

The CJEU ended months of debate over whether ride-sharing company Uber is a transportation company, or an information services provider.

On 20 December 2017, the court ruled that Uber is a transport company in the EU, and will be treated like other taxi companies. Member states will now be able to regulate the conditions for providing that service.

The case was referred by a Spanish judge in August 2015, who asked the court to declare '... whether the firm (Uber) should be considered as a transport service provider or a digital platform'.

## Why is this significant?

The sharing economy – a peer-to-peer business activity through which customers book rides, and rent apartments, bikes, or other commodities directly from taxi drivers and property owners through online platforms – has boomed in recent years. Uber is one of the largest companies operating in this sector; other examples include AirBnb and Lyft.

In particular, Uber's rapid expansion has been accompanied by a wave of legal controversies, including court cases, rulings by regulatory authorities, and decisions by other administrative bodies. Most issues are related to the fact that the sharing economy's business model is still not clearly regulated, even though the CJEU's ruling does shed more light on how the company will be regulated in the EU.

In parallel, the debate on the status of Uber's drivers continues. Companies operating in the sharing economy, or the so-called gig economy, have been criticised for failing to protect the rights of their workers. In countries such as the UK and in some US states, the courts have ruled that drivers are employees, and that Uber must pay their drivers the national living wage, and offer paid holidays, pensions. and other benefits. Many other cases are still pending.

These rulings will affect Uber's business model, and those of other companies within the sharing economy. They will also affect the rights of workers, as courts continue to deliberate, and commissions continue to explore the impact of digitalisation on jobs and the future of work.

**What is Uber in court for?**

In 2017, the *GIP Digital Watch* observatory launched a new study – *Mapping Uber* – which reviewed court cases and rulings by government authorities to determine which issues were contested.

- Of the 50+ cases surveyed, convergence-related issues were predominant in over half of the cases. These include both questions of licensing (taxi companies, largely, arguing that Uber does not have a licence to operate in the region), and classification (asking whether Uber should be classified as a technology company or a traditional taxi service).
- Issues related to labour law were also prominent (24% of the cases). The main question – which remains largely unresolved – is whether Uber drivers are employees or independent contractors. If they are employees – as some courts have already determined – the company would need to offer the same protection and social security benefits to its drivers as any regular employee.
- Competition was a widespread argument used by taxi companies in their cases against Uber involving questions of licensing; issues related to unfair practices include price-fixing, colluding, or misleading practices. These e-commerce-related issues made up around 15% of the cases.

*View the case law: Mapping Uber: Learn more about legal cases and other issues surrounding the ride-sharing company.*

**FOLLOW THE ISSUES**

E-commerce | Other economic issues | Intermediaries | Consumer protection

# #13 Industry prepares for GDPR

The year 2017 was a preparatory year for businesses – including their legal and compliance experts – to put their practices in line with the EU's new GDPR. This will continue in 2018, when the GDPR takes effect on 25 May.

Once in force, the regulation will apply to the personal data of all EU residents, irrespective of where the data is processed or stored. This will be the case both for data controllers (those who decide which data is collected and how it is processed) and data processors (those who hold or process data).

Among the requirements, data controllers and data processors will be asked to implement appropriate technical and organisational measures to ensure the security of the data they process.

If personal data breaches occur, controllers will need to notify the data protection authority, and the affected individuals, if the breach risks having a negative impact of their rights and freedoms.

The concept of 'privacy by design' is now part of the legal framework, as controllers are asked to include data protection features in the design of their systems.

Other new or strengthened provisions in the GDPR relate to concepts such as consent, right to access, the right to erasure (right to be forgotten), and data portability.

## Why is this significant?

One of the most significant changes is the GDPR's territorial applicability, which goes beyond EU borders. The new rules will be applicable to the processing of personal data by entities (controllers and processors) in the EU, irrespective of whether the processing takes place in the EU. Moreover, entities that are not based in the EU, but process personal data of EU citizens, are also required to comply with the new rules if they market goods or services to users in the EU, or monitor users' behaviour.

How entities processing the data of EU residents will actually comply with the new rules, and what changes they will need to make to their current business practices, has long been a matter of debate. For example, when asking for the users' consent, what reasons for processing will Internet companies give them, and how will they accurately distinguish between different flows of data?

It is likely that small and medium-sized companies operating outside the EU will face considerable challenges. This is equally so for companies based in jurisdictions that do not have strong data protection rules.

These challenges will need to be overcome sooner or later due to non-compliance fines. A maximum fine of 4% of the entity's annual global turnover or €20 million (whichever is greater) is a steep price to pay.

### Reconciling the GDPR with domain name registrants' data requirements

The path to GDPR implementation has not been entirely smooth. For ICANN, this has meant a reconciliatory exercise between the GDPR provisions and the so-called WHOIS policy.

ICANN has several agreements with registries of generic top-level domains (gTLDs, such as .com and .net) and registrars of domain names (entities through which end-users register domain names). Traditionally, these agreements have included obligations for registries and registrars – based in many different jurisdictions around the world – to collect and make publicly available certain data of domain name registrants. One of the uses of such data is to assist law enforcement authorities in curbing criminal activity.

Over the past year, ICANN has tried to determine how to reconcile these requirements with the GDPR provisions. It has not yet reached a conclusion, but in November 2017 it decided to enforce a temporary solution: It would not to take action against registries and registrars for non-compliance with the WHOIS policy, under certain conditions.

**FOLLOW THE ISSUES**

Privacy and data protection | Jurisdiction | Consumer protection | Other economic issues

# #14 Taxation pressures increase for Internet companies

Internet companies worldwide are under increased pressure to 'pay their fair share' of taxes. Australia announced a 10% goods and services tax on digital products and services from overseas that are bought in Australia; in Russia, a Google Tax Law similarly obliges foreign Internet companies to pay value-added tax on sales of online services; and Israel is planning to send tax bills to Google and Facebook. Other countries have decided to make deals with Internet companies on their tax bills, such as Italy and Indonesia, which both agreed on tax settlements with Google.

More comprehensive Internet tax proposals were announced in the framework of the EU. France, Germany, Italy, and Spain proposed that companies be taxed on their turnover, as opposed to their profits. In a different proposal, based on the same philosophy, Estonia pushed the idea of taxing profits based on the notion of virtual permanent establishment.

The proposals came after a French court ruled, in July 2017, that Google was not liable for back taxes on advertising revenues in France. Although the adverts were displayed in France, they were booked through a subsidiary in Ireland; the tax bill was therefore not justified, as Google did not have a 'permanent establishment' or 'sufficient taxable presence' in France. Governments continued their discussions during the autumn at EU Summits, and G20 and OECD meetings, among others.

## Why is this significant?

Perhaps the best-known recent tax case in Europe is the Apple/Ireland 'sweetheart tax' ruling, in which the European Commission ordered the company to pay the Irish state up to €13 billion in taxes in August 2016. This ruling, as well as more recent court cases and new government tax proposals, show how authorities are increasingly uncomfortable with companies taking advantage of low-tax-rate countries in which to establish their subsidiaries.

Complicating the issue is the fact that goods and services offered by the Internet giants in so many jurisdictions are largely varied, rendering the attribution of profits and coordination between tax authorities a challenge. Existing tax rules may not be adequate for today's digital economy. The debates in Europe showed a clear rift between governments who are keen on companies paying taxes, and others who stand to benefit more from the status quo. The idea of a two-stepped EU – by allowing, for example, simplified legislative procedures to avoid vetoes – has already been floated.

In parallel with developments at EU level, officials are waiting for the OECD's interim report on tax challenges of digitalisation, due in April 2018. EU officials, however, have indicated that they would be willing to go ahead if progress is stalled; the Commission's proposal on digital taxation is due in March 2018.

**In brief: Tax-avoidance strategies explained**

One of the ways in which companies avoid taxes is through the 'Double Irish' and the 'Dutch Sandwich' arrangements, according to a report from Bloomberg. This involves shifting revenues from an Irish subsidiary to a company in the Netherlands with no employees, and then on to a Bermuda mailbox owned by another Ireland-registered company. Although Ireland has closed its tax loophole, companies already using this structure can continue using it until 2020.

## Which companies hold the most money offshore?

The annual study by the US Public Interest Research Group confirms, year after year, that Internet companies are among the top 10 US companies with the most money held offshore.

*(The numbers in brackets: Amount held offshore in millions $)*

| 2015 | | 2016 | | 2017 | |
|---|---|---|---|---|---|
| APPLE | (181,100) | APPLE | (214,900) | APPLE | (246,000) |
| MICROSOFT | (108,300) | MICROSOFT | (124,000) | MICROSOFT | (142,000) |
| GOOGLE | (47,400) | GOOGLE | (58,300) | GOOGLE | (60,700) |


FOLLOW THE ISSUES

Taxation | Intermediaries | Other economic issues

# #15 Net neutrality dealt a blow

Protests in the USA could not prevent the Open Internet Order's fate, when the FCC voted to repeal it on 14 December 2017.

In 2015, the FCC adopted the Open Internet Order, containing rules in favour of net neutrality. The rules allowed the Commission to regulate broadband services as a utility and prohibit broadband providers from introducing unreasonable practices considered harmful to the open Internet: blocking of lawful content, applications, services, or devices; impairing or degrading lawful Internet traffic on the basis of content, application, or service (throttling); and paid prioritisation of certain content, applications, or services.

In early 2017, the FCC's new leadership announced its intention to roll back these rules, as they were believed to harm the further development of broadband infrastructures. The intention materialised with the December vote, and the adoption of the Restoring Internet Freedom Order, which reclassified broadband providers and information service providers, thus limiting the FCC's authority over them.

Under the new rules, Internet service providers (ISPs) are only required to be transparent and to disclose information about their practices to consumers, entrepreneurs, and the FCC.

## Why is this significant?

In the USA, although the new FCC order was welcomed by some (mainly telecom companies), it was heavily criticised by users, businesses, and policymakers.

In the last weeks of 2017, attorney generals in several US states announced plans to challenge the order in court (which they did in January 2018), while lawmakers in states such as Massachusetts, New Jersey, New York, and Washington proposed pro net neutrality bills at state level. In the Congress, senators announced they would introduce the so-called Congressional Review Act resolution to reverse the FCC decision (which they also did in January 2018).

As the year ended, it was unclear what would happen with net neutrality in the USA. The situation clearly attracted attention at international level. Canada and the EU, for example, reaffirmed their commitment to net neutrality, and criticised the change of rules in the USA.

While it was pointed out by many that the new FCC order, once entered into force, would not have a direct effect on how net neutrality is protected in other countries, there could still be an indirect effect. As has been the case in many instances, other countries may choose to follow the US approach.

### What happened in other parts of the world?

While developments in the USA hogged the headlines throughout most of the year, there were updates in other parts of the world as well.

- In November, the Telecom Regulatory Authority of India released a set of recommendations in support of net neutrality – believed to be among the world's strongest rules – following a wide public consultation process that started in May 2016.
- Earlier in the year, the Body of European Regulators for Electronic Communications (BEREC) adopted a *Net neutrality regulatory assessment methodology*, to assist EU national regulatory authorities (NRAs) in monitoring the implementation of net neutrality rules.
- The Canadian NRA released a new framework for assessing differential pricing practices of ISPs, outlining that ISPs should treat data traffic equally to foster consumer choice, innovation, and the free exchange of ideas.
- In Sweden, net neutrality was among the announced priorities of the Post and Telecom Authority, which focused on 'event-driven regulation of ISP's business models'.

**FOLLOW THE ISSUES**

Net neutrality | Telecommunications infrastructure

# #16 Stalemate over WTO's e-commerce mandate continues at MC11

It has long been under discussion whether the World Trade Organization (WTO) mandate should be revised to include e-commerce negotiations. Digital policy issues, such as data localisation, interoperability of standards, or access to the source code, are increasingly framed as trade-related issues, and cannot be separated from trade.

Most developing countries felt that a new mandate to negotiate e-commerce may shift the WTO's energy and time from development issues encompassed in the Doha Round – the latest round of negotiations, started in 2001 and not yet concluded, which focuses on helping developing countries join the global marketplace.

In addition, the digital economy in developing countries is not strong enough to benefit from new e-commerce rules, and there is not enough understanding of the impact that emerging technological developments, such as big data, AI, and 3D printing, will have on e-commerce.

In the lead-up to the WTO Ministerial Conference in Buenos Aires, countries made several proposals, including the creation of a working group (WG) or a working party (WP) on e-commerce, with differing views on its potential mandate.

The conference, held on 10–13 December 2017, ended without producing a final declaration. A group of 70 countries, however, joined together and issued a statement on e-commerce, agreeing to 'initiate exploratory work toward future WTO negotiations on trade-related aspects of e-commerce'.

## Why is this significant?

The stalemate on e-commerce negotiations and a possible change to the existing WTO mandate broadened the dividing lines between developed and developing countries. Discussions on the moratorium on customs duties on electronic transmissions were also stalled, and a renewal of the moratorium was only approved at the last minute. WTO Director General Roberto Azevedo expressed disappointment over the way the negotiations had progressed and called for soul-searching among member countries.

The exploratory work towards future WTO negotiations, as agreed jointly by the 70 countries, could represent a breakthrough in negotiations. The proposals made in the lead-up to the conference still stand, and could become the tangible next steps for an update to the global organisation's mandate.

**What are the main proposals that can lead to a compromise?**

**Clarify applicability of existing WTO rules:** Japan, China, and a few other countries have argued the WG should conduct an evaluation of whether the clarification or strengthening of the existing WTO rules is necessary. Then member states could decide to start negotiations on e-commerce in 2019.

**Create a forum for developing global rules:** According to Russia, the WG would provide members with an appropriate forum for discussions on e-commerce, including the possibility of developing international rules on issues such as scope and definitions of e-commerce, existing applicable rules and gaps in the WTO legal framework, existing barriers to e-commerce, trade facilitation measures, and intellectual property rights.

**Create a framework, avoid silos:** In a joint document, Singapore and more than 15 other countries from several regions have suggested an updated framework or process through which future work could be undertaken.

**Focus on e-commerce for development:** As a potential convergence in negotiations, Costa Rica has proposed an E-Commerce for Development Agenda, which would assess the needs, challenges, and priorities of developing countries, under a joint effort by UN agencies.

*Review the countries' positions in more detail.*

**FOLLOW THE ISSUES**

**E-commerce** | **Other economic issues** | **Access** | **Development**

# #17 Cryptocurrency's volatility confirmed as regulators step in

On 17 December 2017, Bitcoin's value reached a record-high of $20,089. It soared by over 300% in just one month, and fell back to $12,633 by the end of the year. Bitcoin's value at the start of the year was just under $1,000. The year, therefore, confirmed the cryptocurrency's volatility.

There have been mixed reactions by countries on how to deal with cryptocurrencies. In 2017, Japan recognised Bitcoin as legal tender, while Malta proposed that Europe should become the Bitcoin continent, as 'some financial institutions are painstakingly accepting the fact that the system at the back of such transactions is much more efficient and transparent than the classical ones.' Russia, on the other hand, urged for more regulation, citing concerns over money laundering and tax evasion.

Belarus adopted a new cryptocurrency law which legalises Bitcoin, and regulates Initial Coin Offerings (ICOs), online exchanges, and transactions in cryptocurrencies. This placed Belarus at the forefront of other countries in regulating the sector, and the third European country to legalise crypto industry products (after Switzerland and Luxembourg).

In the USA, cryptocurrency exchange Coinbase was ordered by a Californian federal court to report users who moved more than $USD20,000 in online exchanges – around 15,000 of the exchange's users – to the Internal Revenue Service (IRS). Transactions in the Bitcoin system are transparent, but only Coinbase has the required data to identify the owner of each account, which is necessary for assessing the user's tax status.

Regulators also reacted to the cryptocurrency crowdfunding phenomenon of ICOs – used by startups to attract investment through new cryptocurrencies. In September 2017, China banned ICOs and ordered the return of any investments made through ICOs. Later in the year, the European Securities and Markets Authority (ESMA) warned companies and investors of the main risks involved, from loss of investments and the lack of adequate information on products developed, to the possibility of technology flaws since the distributed ledger technology (blockchain) is still largely untested.

## Why is this significant?

Volatility is one of the main concerns for governments, as consumers could suffer huge losses when values plummet. Security risks also increase when values soar. Since cryptocurrency is unregulated, consumers do not have any protection.

Yet, the demand for cryptocurrency has been on the increase: consumers are drawn to the novelty, while startups are jumping on the bandwagon of attracting investment through new cryptocurrencies.

ICOs are also a concern for governments. They present significant risk since they do not undergo the auditing and regulatory scrutiny which initial public offerings go through. In addition, ICOs could be fraudulent.

Governments seeking to regulate cryptocurrency also have tax evasion and money laundering issues in mind. Imposing obligations on cryptocurrency exchanges (the equivalent of a foreign exchange) to collect taxes may be considered by governments after a Californian federal court ruled, in November 2017, that the exchange Coindesk is obliged to forward customer details to the IRS.

Although the ruling applies only to transactions over US$20,000 made during 2013–2015, it inches authorities closer to enforcing rules on a decentralised system.


**FOLLOW THE ISSUES**

E-Money and virtual currencies | Cybercrime | Jurisdiction

# #18 Blockchain, moving beyond Bitcoin?

Blockchain technology offers many potentials, and yet, it has had a limited impact so far. Initially, it was often identified with Bitcoin; later in 2017, blockchain mainstreamed into the language and thinking of many organisations and companies.

The technology has the potential to revolutionise the way the Internet functions by re-introducing the idea of a decentralised network. This was indeed the idea behind the origins of the Internet: peer-to-peer networking is now enjoying a renaissance through new online decentralised business models.

These new solutions are still waiting for global acceptance, since the power of decentralisation lies in being adopted on a massive scale. Blockchain supporters believe that this process will take time, and that in the interim there will be many disappointments, including the potential failure of some cryptocurrencies.

## Why is this significant?

The impact of blockchain – which was believed would significantly affect traditional industries such as insurance, healthcare, energy, retail, and real estate – has not yet translated into breakthrough applications.

Blockchain for social change has also not yet progressed. Its uses would include blockchain voting, decentralised democracy mechanisms, improvement of land records, online privacy, or personal identification for refugees. The scaling of blockchain networks is one of the most visible limitations.

At the same time, there are many positive examples of the use of blockchain, mostly from the financial sector. Financial institutions have been implementing blockchain solutions for cross-border payments, and for clearing settlements. For example, IBM partnered up with blockchain startup Stellar for cross-border payments in southeast Asia.

Although it is currently limited to transactions in sterling, the platform is designed to handle seven fiat currencies from the South Pacific, including the Australian dollar, the New Zealand dollar, and the Tonga pa'anga. The Ripple technology seemed to capture the trust of leading banks and financial industries for cross-border payments.

**How is blockchain administered?**

Blockchain can be open (permissionless), private (permission-based), or a combination of open/private (some parts are open, other need permission to access).

This trichotomy has created a wide range of possibilities using different security and privacy models. Companies that utilised older online business models have mostly been using blockchain as a distributed data ledger with permission-based access. New business models emphasise the network effect and decentralised approach through open blockchains.

**FOLLOW THE ISSUES**

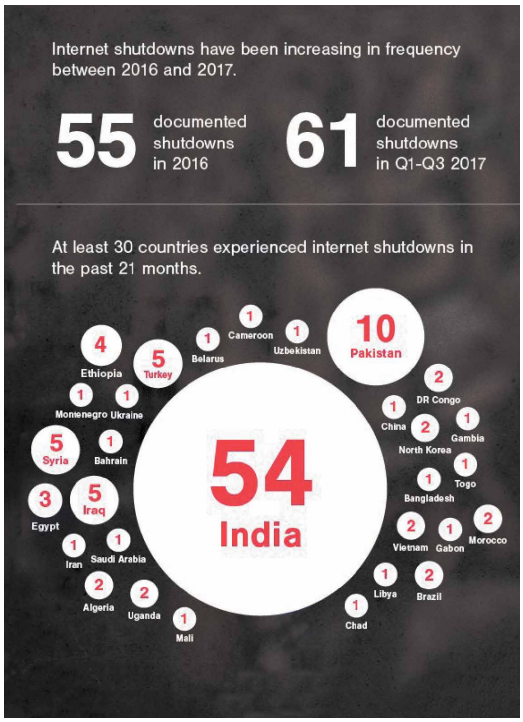
E-Money and virtual currencies | Other economic issues

# #19 Internet freedom in decline as shutdowns increase

If 2016 saw a decline in Internet freedom – obstacles to access, onerous restrictions on content, or violations to freedom of speech – 2017 saw an even further deterioration. The Freedom of the Net 2017 report revealed that nearly half of the 65 countries assessed (covering 87% of the world's Internet users) experienced an abuse of Internet freedom. Less than one-quarter of users reside in countries where the Internet is designated free.

The report also confirmed new trends: social media is being manipulated to undermine democracy; shutdowns are increasingly directed at mobile Internet services; governments are restricting live video; cyber-attacks against journalists and physical attacks against online journalists are on the increase, as are restrictions on virtual private networks.

By September 2017, AccessNow's Shutdown Tracker Optimization Project found that the number of shutdowns had already surpassed the number recorded in 2016. India and Pakistan, Turkey, Syria, and Iraq were the countries which experienced the most shutdowns. Cameroon's Internet shutdown lasted over three months. In some countries, such as Iran, shutdowns are showing increased technical expertise in targeting and carrying out government controls.

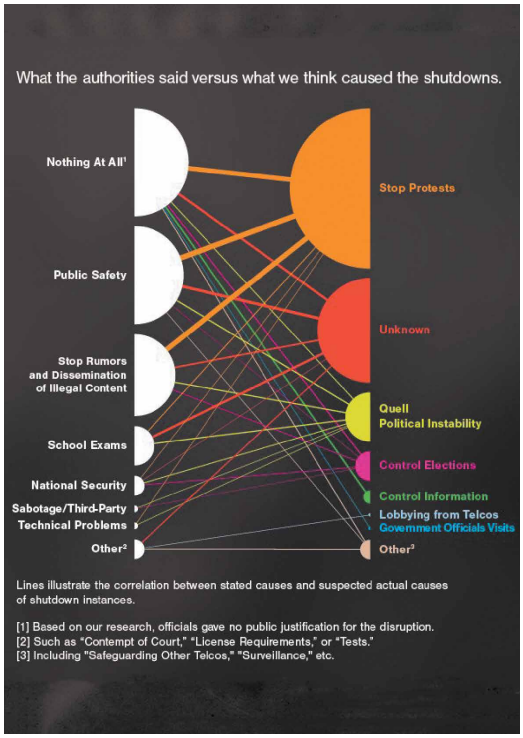



## Why is this significant?

In addition to the obvious profound impact of lack of access to information and communications, misuse of the digital public policy space, including social media, can lead to so-called information disorder and the distortion of 'truth', mistrust in public information, and misrepresentation of public opinion. Although not a new phenomenon, the spread of misinformation on social media has made it more difficult to distinguish between verified or false facts and opinions.

Internet shutdowns have major social and economic impacts. The Internet shutdown in the anglophone region of Cameroon – which lasted for 93 days – was one of the most widely discussed global shutdowns of 2017. In the same region, social media and messaging apps were blocked for over six months. What did this mean for users? 'In countries like Cameroon, shutting down social media and messaging apps de facto equals shutting the whole Internet.'

Restrictions on virtual private networks (VPNs) and anonymisers, most notably in Russia, and China, mean that users will be unable to use the few remaining avenues to access the global Internet. The crackdowns are part of new legislation that raised concern over new levels of Internet censorship.




**FOLLOW THE ISSUES**

Access | Digital divide | Privacy and data protection | Freedom of expression | Other economic issues | Intermediaries

# #20 IGF discussions turn to core values

The digital policy year can be said to have ended with the 12th Internet Governance Forum (IGF), on 18–22 December 2017, in Geneva. The meeting explored a wide range of digital policy issues, from data, cybersecurity, and digital commerce, to AI and other frontier issues.

In many of these discussions, the focus turned to core human values, such as 'democracy', 'trust', 'freedom', and 'community'. These were among the most frequently used words at this year's IGF, including in the context of call for actions on how to best 'shape our digital future'. As one of the *Geneva Messages* indicates, 'While we cannot predict how our digital future will look like, [...] we should take a human centric and ethics-based approach to digital development.'

## Why is this relevant?

The digital future is indeed uncertain, but the way in which we address today's challenges will surely impact it. We might not know what challenges we will face 20 years from now, but we know, for example, that digitalisation and automation processes will bring changes to the labour market. And we know that cyber risks are here to stay as long as there is a cyber space.

This year's IGF looked closer at how these and other challenges can be tackled. There were many calls for actions, from addressing cybersecurity risks in a more concerted manner, to assisting developing countries in their digital development efforts, and to better integrating women and gender minorities in the digital society.

The *Geneva Messages* showed that, when we look at our digital present and future, the glass is half-full. If we guide ourselves by the same human values that have been at the core of our evolution, we can shape a promising digital future and achieve a widely acceptable digital social contract.

### In focus: Values integrated into calls for actions

How do we shape our future digital global governance? This was the focus of a high-level session at the IGF, in which participants said that effective digital governance needs to adapt and respond to the needs of the world's citizens. It should also be value-based, inclusive, open, transparent, and human-centred.

During the main session on cybersecurity, there was broad agreement that cyberspace needs to be preserved as a place for peace, stability, and prosperity, and, for this to happen, cooperation within and between stakeholder groups needs to be enforced. Views differed on whether we need – or whether it is feasible to develop – new international treaties or conventions to encode rules, norms, and principles for cybersecurity.

Similarly, participants in the main session on digital transformation discussed both the opportunities and risks from developments in AI and automation. Ethics and humanity need to be placed at the core of both technological progress and policy approaches for maximising the opportunities and tackling the risks.


Published on 10 January 2018

IGFREPORT

FINAL REPORT FROM THE 12th INTERNET GOVERNANCE FORUM

dig.watch/igf2017

*IGF 2017 Report* prepared by the Geneva Internet Platform with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation

Reflecting on IGF 2017: The values at the core of our digital future

If the Internet is a mirror of society, as Vint Cerf argued, the Internet Governance Forum is a mirror of global digital politics.

IGF 2017 reflected on a very turbulent year in global politics, with a number of issues resonating throughout the week: values on the Internet, digital future and frontier issues, dealing with data, cybersecurity and digital commerce, and the need for action and capacity development.

Perhaps succeeding better than in the real world, many convergences were created at the IGF, as the *Geneva Messages* indicate. However, differences emerged as the discussion moved from principles to concrete action and details. For example, while there is shared understanding of the need for action in cybersecurity, there are differences as to whether this should be done gradually through existing law, or through major action with the adoption of a cyber treaty.

Among the most frequently used words at this year's IGF, many relate to human values, such as 'community', 'democracy', 'trust', and 'freedom'. Values came into focus in many discussions on artificial intelligence (AI), fake news, the role of Internet companies, human rights, and others.

Continued on page 2 and 3



The opening ceremony of IGF 2017, on 18 December. Credit: UN Photo/Jean Marc Ferré

IN THIS ISSUE



Click on the icons in the digital version to access session reports and additional information.

**FOLLOW THE ISSUES**

Infrastructure | Security | Human rights | Legal | Economic | Development | Sociocultural

# Stay on top of #digitalpolicy

Follow **the latest developments across 40+ Internet governance topics** including cybersecurity, infrastructure, privacy, artificial intelligence, and blockchain | **https://dig.watch**

Keep track of **upcoming global policy events** and use DeadlineR to remind you of important events and dates | **https://dig.watch/events**

Join the **digital briefing on the last Tuesday of every month (13.00 CET)** for a summary of global policy developments | **https://dig.watch/briefings**

Read **in-depth analysis of digital politics in the monthly newsletter**, in English, French, Spanish, Portuguese, or Bahasa Indonesian) | **https://dig.watch/newsletter**

Learn about digital policy via **just-in-time and online courses** on Internet governance, cybersecurity, digital commerce, and other topics | **https://www.diplomacy.edu/courses**

Engage in **conceptual and policy discussions about the digital world** at Geneva Internet Platform (GIP) conferences and other events | Develop your **digital policy network** with diplomats, policy experts, and digital entrepreneurs at the GIP | **Venue: Geneva Internet Platform, WMO, Av de la Paix, Geneva**

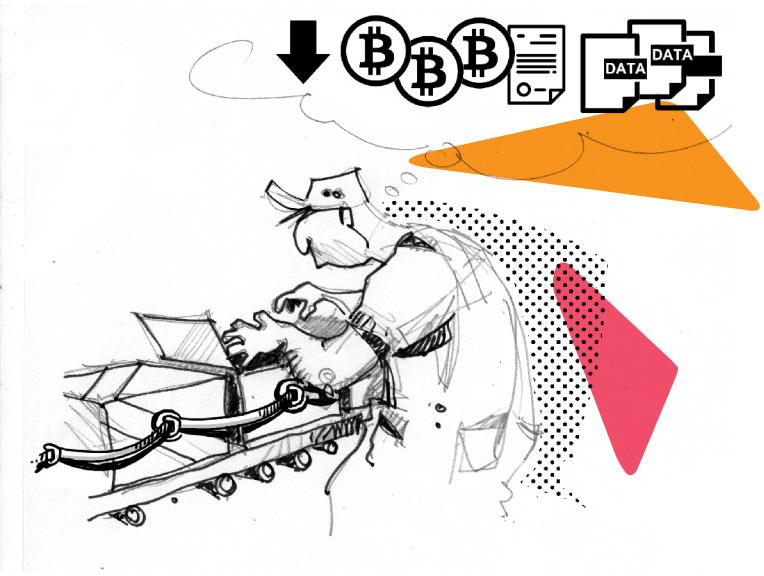
Geneva Internet Platform

The GIP is operated by DiploFoundation (Diplo) with the support of its founding members: the Swiss authorities (the Federal Department of Foreign Affairs of Switzerland and the Federal Office of Communications - OFCOM), the University of Geneva, ETH-Board, and DCAF.

The GIP and Diplo have worked with, among others, the Internet Society, the Internet Governance Forum Secretariat, Canton de Genève, the Geneva Center for Security Policy, the Internet Corporation for Assigned Names and Numbers, the UN Office in Geneva, the International Telecommunication Union, the International Trade Center, UNCTAD, Swissnex - San Francisco, the African Union, the Asia-Europe Foundation, the governments and permanent missions of Argentina, Finland, Indonesia, the Netherlands, Namibia, Macedonia, Malta, Mexico, Paraguay, South Africa, Switzerland, United Kingdom, and United States, the Commonwealth Small States Office, the University of St Gallen, the College of Europe, CUTS International, ICT for Peace, Foraus, Association for Proper Internet Governance, and more.

**Contact us for joint activities and partnerships**

Geneva Internet Platform | gip@diplomacy.edu | Avenue de la Paix 7bis, Geneva | tel. +41 22 730 8625

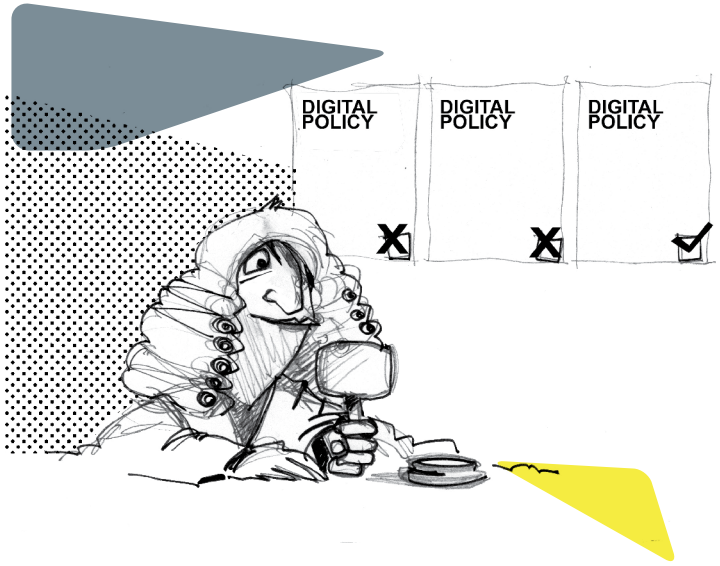



## JANUARY 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

## FEBRUARY 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |





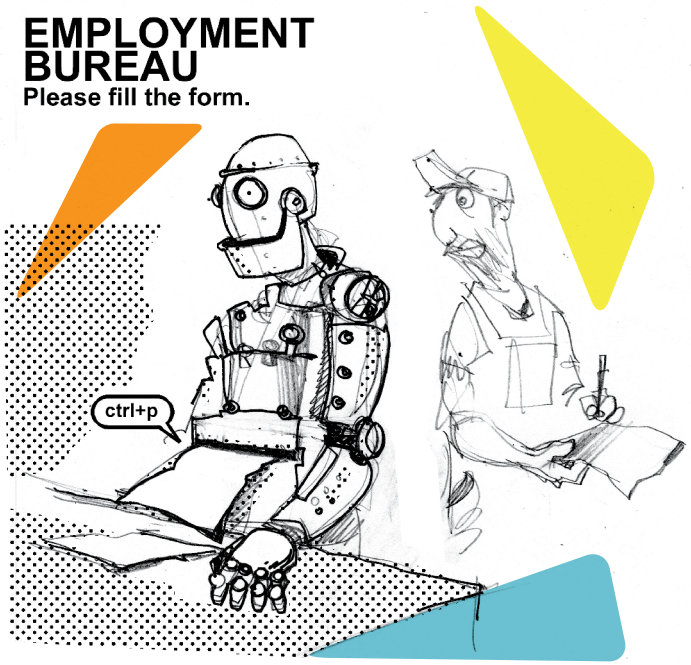
## MARCH 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |

DiPLO
www.diplomacy.edu

## APRIL 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 1 | 2 | 3 | 4 | 5 | 6 |



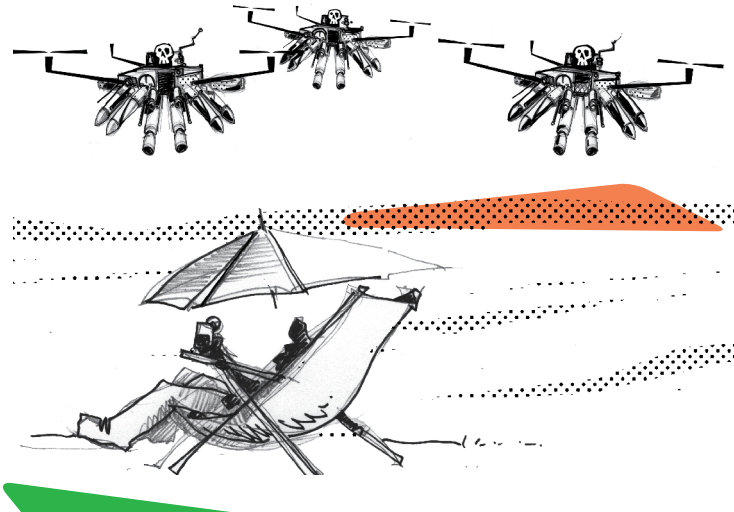


## MAY 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 30 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 31 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |

## JUNE 2018

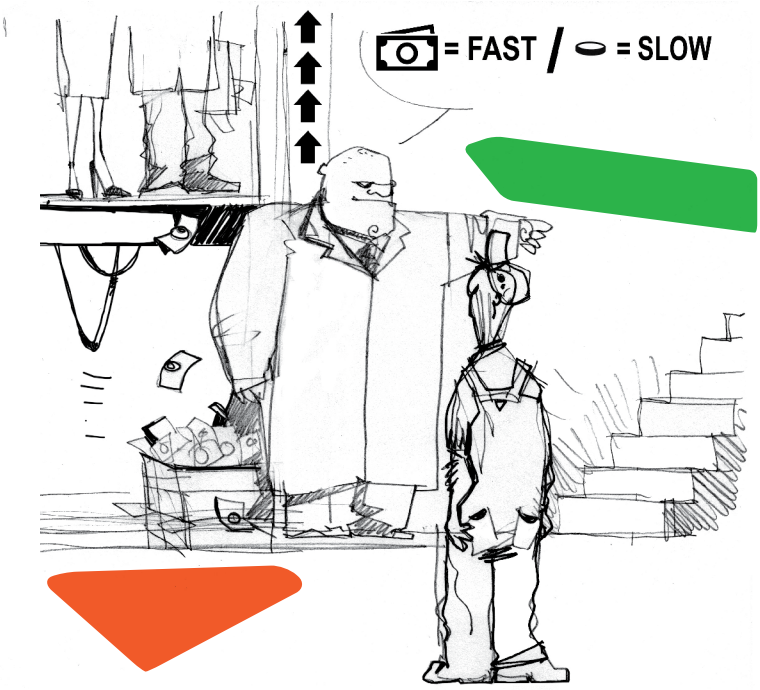
| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 28 | 29 | 30 | 31 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |



DiPLO
www.diplomacy.edu

## JULY 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 25 | 26 | 27 | 28 | 29 | 30 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | 1 | 2 | 3 | 4 | 5 |

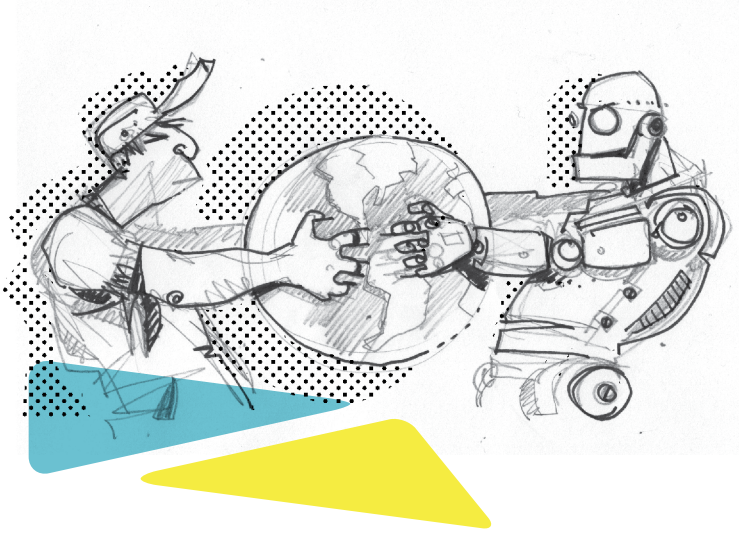



## AUGUST 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 30 | 31 | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |

## SEPTEMBER 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 27 | 28 | 29 | 30 | 31 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |



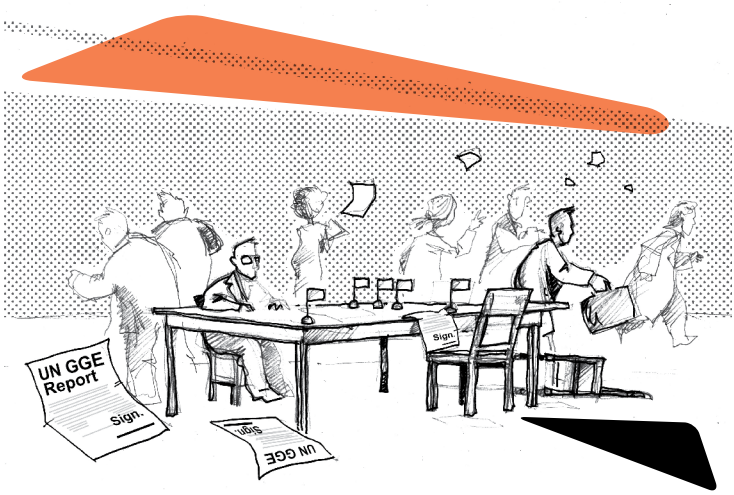
DiPLO
www.diplomacy.edu


## OCTOBER 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

## NOVEMBER 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |





DiPLO
www.diplomacy.edu

## DECEMBER 2018

| Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 29 | 30 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |