Geneva Internet Platform
DigitalWatch
dig.watch

Issue 39, April 2019
Newsletter

# 5G geopolitics: A game of e-thrones

## TRENDS IN APRIL

Misinformation is a major concern for upcoming elections. Internet companies face more pressure.

*More on page 2*

## FROM THE OBSERVATORY

Security, privacy, e-commerce, digital rights, and legal issues are perennially prominent.

*More on pages 4–5*

## IN FOCUS: HUAWEI

As the controversy over 5G products wages on, the politicised battle reveals a deeper side.

*More on pages 6–7*

## DATA ANALYSIS: AI STRATEGIES

A handful of countries have developed national AI strategies. We dissect them to find out what they have in common.

*More on pages 8-9*

# The top digital policy trends in April

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 month.

## 1. Upcoming elections trigger fresh concerns over misinformation

Misinformation continues to be one of the biggest issues this year. It strikes at the heart of democracy, affecting elections and facilitating foreign interference in domestic affairs.

One of the tools to fight it is to know who is behind political adverts. Ahead of India's general elections on 17 May, Facebook's updated policy strategies will require advertisers to confirm their identity, and citizens will be able see who has placed (and paid) for adverts. The company has also set up regional operation centres for speedy remedial action to alerts.

Yet, Facebook's updated strategies may not work well in every region. In Europe, the EU Commission asked the company to rethink its strategy ahead of the European Parliament elections (23–26 May 2019). In a region where cross-border campaigns are meant to target audiences across every member state, the rules which require advertisers to register in every country may be hindering the exercise of electoral rights, and therefore breaching EU law.

**The three untruths**

These terms are often used interchangeably, but there are more than subtle differences between them.

- Disinformation is information that is false and deliberately created to harm a person, social group, organisation, or country.
- Misinformation is information that is false but not created with the intention of causing harm.
- Mal-information is information that is based on reality, used to inflict harm on a person, social group, organisation, or country.

Source: UNESCO's Handbook on Journalism, Fake News and Disinformation (2018).

Beyond elections, the recent terror attacks in Sri Lanka drove the government to cut access to social media, messaging services, and virtual private networks (VPNs) to prevent the spread of misinformation and any further violence. This was in reaction to the dangerous spread of content naming the perpetrators of the Easter Sunday attack (21 April), before the information was verified by authorities.

In Singapore, a new law will criminalise the publication of 'fake news', and will allow the government to order its removal.

The main challenge is how to balance freedom of expression with the need to prevent the spread of misinformation. Speed and time are increasingly important factors. If misinformation is able to spread as quickly as wildfire, the need for concerted action needs to happen just as fast.

## 2. New data breaches, more pressure on companies

Data breaches make the news regularly. In April, cybersecurity firm UpGuard uncovered two large troves of exposed Facebook user data of about 500 million users, posted publicly on Amazon cloud servers. Another privacy breach revealed that Facebook harvested the private data of 1.5 million users without their consent.

This contrasts starkly with Facebook's recently announced plans for a privacy-focused app. Gaining credibility and support is important for the tech giant, especially in light of its plans to provide services and accept payments through the app, and take a cut. Nevertheless, this will not be easy, given the countless breaches of private data. Even if we accept that users willingly trade their private data in return for free services, data breaches are surely not part of this 'tacit deal' between users and tech companies.

In an opinion piece published in The *Washington Post*, Facebook's CEO Mark Zuckerberg called for tighter regulation of Internet companies. Privacy is one of four areas that are most in need of regulation: 'People around the world have called for comprehensive privacy regulation in line with the European Union's General Data Protection Regulation, and I agree. I believe it would be good for the Internet if

more countries adopted regulation such as GDPR as a common framework.'

The UK's Information Commissioner, Elizabeth Denham, called out Zuckerberg to walk the talk on the GDPR. Referring to Facebook's appeal against. the Information Commissioner's Office fine in the Cambridge Analytica case: in light of Mark Zuckerberg's statements... I expect Facebook to review their current appeal against the ICO's £500,000 fine.'

Although by supporting GDPR-style rules one does not forfeit any right to appeal, Facebook's next step will be used as a measure of its intentions.

### 3. Digital health in focus

Digital health refers to all areas of healthcare where technology is used to impact people's health, whether on an individual level (e.g. through wearables), or on a national level (e.g. digital health national strategies, and policies on the protection of health data).

While once on the periphery of more mainstream digital policy areas, digital health has since gained prominence with the introduction of new regulations and strategies. The recent guidelines by the World Health Organization, on how countries can use digital health technology to improve people's health, offers new ideas. For instance, births could be registered through mobile phones, and health professionals can benefit from online training.

The Geneva-based organisation, which last year classified gaming addiction as a disorder, is also tackling the wellbeing of children, and has offered guidelines on the amount of screen-time for children. A sedentary lifestyle, even for young children, can impact their physical and mental wellbeing. WHO recommends that children under the age of five limit their screen-time and non-active behaviour in favour of more active playtime.

When it comes to health data, the Council of Europe recently issued a new set of guidelines for the protection of sensitive data in line with its recently update data protection convention.

Since digital health is a growing market, and continues to be one of the most highly attacked sectors, legislation and policy on health data will need to ensure that the data is adequately protected from cyberattacks, breaches, and other risks.

Digital health is attractive for start-ups and other companies, which are now investing heavily in it. Digital technologies, entrepreneurship of the private sector, and involvement of the medical professionals can make healthcare more accessible, affordable, and secure.

*Credit: IBM Research*

# Digital policy developments in April

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

UNCTAD published its new Rapid eTrade Readiness Assessments for least developed countries, which analyses the barriers to e-commerce and digital trade development for specific countries.

same relevance

## Sustainable development

Achieving the sustainable development goals (SDGs) hinges on overhauling national and international financial systems, according to the latest report of the UN Inter-agency Task Force on Financing for Development. The potential of emerging technologies, and the support which developing countries need to harness this potential, are also explained in the report.

increasing relevance

## Security

G7 foreign ministers adopted the Dinard Declaration on the Cyber Norm Initiative, which encourages voluntary exchange of information, best practices, and lessons learned on implementation of voluntary, non-binding norms of responsible state behaviour.

Russian President Vladimir Putin signed the law on providing a stable operation of the Russian Internet (Runet), which should ensure a 'sustainable, secure, and fully functioning' Runet in case it is disconnected from the global infrastructure of the World Wide Web (WWW). The law is set to take effect on 1 November 2019.

increasing relevance

## E-commerce & Internet economy

The European Commission's report on Competition Policy for Digital Era calls for new antitrust rules for tech giants. It suggests improving legal certainty in the digital market, such as improved definitions of 'dominance' in the digital environment.

The European Parliament approved new online platform rules aimed at curbing unfair practices and increasing the transparency of their trading practices.

China is considering shutting down cryptocurrency mining operations and banning investments and loans in this field, as the industry is 'polluting the environment; and 'wasting energy'.

increasing relevance

## Digital rights

Wikileaks founder Julian Assange's political asylum was revoked by the Ecuadorian Embassy. He was arrested by UK police, sparking concerns about freedom of expression and threats to journalism.

The European Parliament voted for a biometrics database for border management called Common Identity Repository (CIR), which will interconnect identity and biometric records of EU and non-EU citizens into one massive, searchable database. Jamaica's Supreme Court declared the national biometric identity law unconstitutional as it abrogated the right to privacy.

increasing relevance

## Jurisdiction & legal issues

EU Copyright Directive received final approval by the European Council.

Facebook will improve its 'reduce, remove, inform' approach against fake news by establishing a 'Quality Group' feature to hold group administrators more accountable for conduct towards illicit content shared within the group.

Australia passed a strict intermediary liability law making it a criminal offense for social media platforms to fail to promptly remove violent user-posted material.

The UK government published its Online Harms White Paper which calls for an independent 'online harms' regulator with effective enforcement powers, such as the power to issue fines and block access to sites.

same relevance

## Infrastructure

Controversy over Huawei's 5G equipment wages on, amid leaks and possible investigations. The newest case comes from Serbia where concerns about Huawei's Safe City Solution for Belgrade are being raised.

Investment in undersea cables by private companies continues as Google completes the Curie cable from the USA to Chile and Infinera upgrades Orange's Kanawa subsea cable in the French Caribbean.

decreasing relevance

## Net neutrality

A new bill which will restore net neutrality rules that prohibited blocking, throttling, and paid prioritisation titled 'Save the Internet Act' was approved by the US House of Representatives.

An increase in blocked websites in India despite net neutrality laws has raised questions about the enforcement of said laws.

increasing relevance

## New technologies (IoT, AI, etc.)

AI researchers have signed a letter calling on Amazon to stop selling facial-recognition technology to law enforcement agencies.

The EU High-Level Expert Group on artificial intelligence published ethics guidelines for the development and use of trustworthy AI.

Google opened its first AI centre in Ghana to provide researchers with the necessary tools to build AI products that are adjusted to the needs of the African economy.

# Controversy over Huawei's 5G products wages on

**As predicted for 2019, hardware remains important in geopolitics. The 2018 controversy around Huawei, which started with the USA banning use of its products in government networks, and continued with the arrest of its CFO by the Canadian authorities, has picked up again. What's behind it?**

Media reports speculate whether President Trump will sign an Executive Order to ban Huawei's products from telecom networks in the USA, a decision likely connected to trade negotiations with China. The Department of Justice has accused the firm of intellectual property theft and of being untruthful about its compliance with US sanctions of Iran.

Australia, Japan, and New Zealand have taken measures to prohibit or limit the use of Huawei's products in their networks. Yet, after in-depth scrutiny of its products and much internal debate, Germany has decided not to ban them and the UK has decided to allow Huawei to supply its 5G network only with non-core components. In response, the USA has warned both Germany and the UK that it will limit intelligence sharing as a result.

As the USA increases pressure on key European allies to follow suit, and as the EU expresses concern about Huawei's possible co-operation with the Chinese Secret Service, the controversy is becoming increasingly geopolitical.

For instance, the 5G Security Conference in Prague, attended by 32 OECD and other countries, further confirms the changing geopolitical landscape. Without explicitly referring to the company, the non-binding Prague Proposals – the main outcome of the conference – spell Huawei, nonetheless.

## Huawei mired in security concerns

The USA argues that Huawei's products threaten national security. Embedded 'backdoors' – intentional flaws in the software code or product design – may allow Chinese authorities to either spy on, disrupt, or destroy the network capabilities of their political or corporate opponents. Of particular concern for US officials is 5G network security, which is intended to be the backbone of the more advanced Internet of Things (IoT).

Even though no evidence of backdoors is publicly available so far, the existence of backdoors is not excluded. Technology is largely a black box: vendors safeguard trade secrets to retain competitive advantage and are often not fully aware of every software or hardware flaw that exists, or those that may have been inadvertently – or intentionally – overlooked. Software solutions, in particular, contain flaws. A relatively simple application such as a web browser has over 5 million lines of code, and even the smallest error in the code can enable a third party to exploit the intended use.

In this regard, Huawei's products are no different. The company's products could contain backdoors, and they certainly contain unintentional vulnerabilities – much like other digital products, including those of Huawei's competitors.

A few companies, such as Microsoft, Kaspersky as of recently, and now Huawei, allow their code to be scrutinised by partner countries in insulated environments. As a precondition to being allowed to continue operations in the UK, Huawei's Cyber Security Evaluation Centre, set up in the UK, is staffed by company employees as well as technical experts from the UK's intelligence service GCHQ.

## Behind the controversy: Market-share woes

But is security the main reason behind calls for banning Huawei, or is it more about market dominance? Who will get to the throne first?

*The Economist* believes it is an economic concern: 'The arguments are about more than coding. Huawei is a Chinese champion. As an aspirant superpower, China sees technology as a vital national interest. The incumbent superpower, America, thinks similarly and a technological cold war is developing between the two.

Huawei has been investing heavily in developing countries, such as the West Africa Cable System and Thailand's 5G test bed. It has also been investing in Europe in co-operation with major telecoms, for example in Spain and Monaco, and particularly with regard to the roll-out of 5G networks.

Huawei – and other Chinese tech companies – are therefore being seen as taking too much of the global market share, challenging the power of the US-based tech industry.

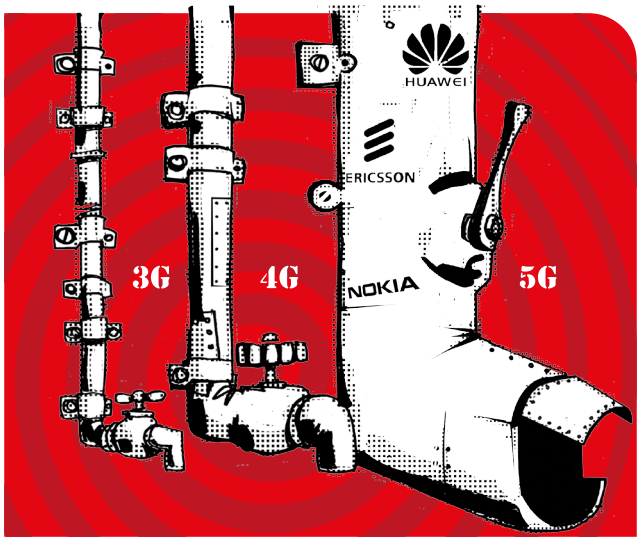
## What lies ahead?

Although the trade war between the USA and China will most likely intensify, it remains to be seen if China will retaliate and ban US products such as Apple and Cisco.

The position of European economies may be decisive for the future of this debate. Europe aims to become a frontrunner in 5G as an enabler of the Internet of Things. Delays in the deployment of 5G due to a possible Huawei ban could cause strategic disadvantage but also result in financial loss: a recent study commissioned by UK mobile operators estimates that, while the benefit to the UK economy of a timely 5G roll-out would be around £164 billion by 2030, the cost of a delay would be between £4.5 and £6.8 billion. In addition, in the event of a Huawei ban across Europe, its main European competitors namely Nokia and Ericsson – and other industry leaders may be pushed out of China, which would be a big blow to their business.

The prevailing consideration is not just who to trust, but even more, who offers a better deal. The telecom sector will likely remain pragmatic and business-oriented, and continue co-operation with Huawei and others; many governments will probably support this.

To maintain a presence in the key developed markets of the West, this highly politicised controversy could force big vendors to be more transparent as to what their 'black-box' products contain. Huawei has already taken a step in this direction by opening its Cyber Security Transparency Centre in Brussels. Vendors could regain the trust of their consumer-countries by agreeing to be scrutinised by their security agencies; if this takes off in Europe, it could become an important security trend.




### Prague's 5G Security Conference: What went on?

Following two days of discussions, the 5G conference in Prague, which gathered officials and experts of EU, NATO, and OECD states, announced the Prague Proposals, a set of non-binding proposals dedicated to the security of 5G networks.

The adoption of the proposals was prompted by the lack of a co-ordinated approach by EU, NATO, and other partner countries to ensure the security of future 5G networks. The Prague Proposals express concerns that equipment supplied by vendors might be at risk of being influenced by a third country, especially if that country does not follow policy and rules set in cooperation agreements on cybersecurity, cybercrime, or data protection.

The document clearly shows a shift in narratives – from global to national. For instance, the proposals state that international frameworks should be flexible enough to allow security concerns to be addressed at a national level. Increasingly different national approaches will heighten the importance of digital international cooperation.

However, this shift might also signal a crisis (or even the end) of digital liberalisation. The success of Huawei could drive countries to regulate the current liberal telecoms market, as a trade-off for security. The aftermath of this case is extremely relevant for Europe, as Austria, Belgium, the Czech Republic, France, Germany, Greece, Hungary, Ireland, the Netherlands, Lithuania and Portugal are preparing to auction 5G licenses this year.

# Dissecting AI strategies

**A handful of countries have developed national artificial intelligence (AI) strategies. More are following suit. A deeper look at these strategies shows areas of commonality and divergence.**

AI, an umbrella term now often used to refer to machine learning, computational neuroscience, and deep learning, is no longer a product of the vibrant imagination of science fiction writers, or a topic that only preoccupies the attention of the scientific community. AI applications – from smart personal assistants to driverless cars – are becoming part of our daily reality. As AI climbs national and international policy agendas worldwide, some countries are also vying for AI dominance.

## Six percent of countries have developed national strategies

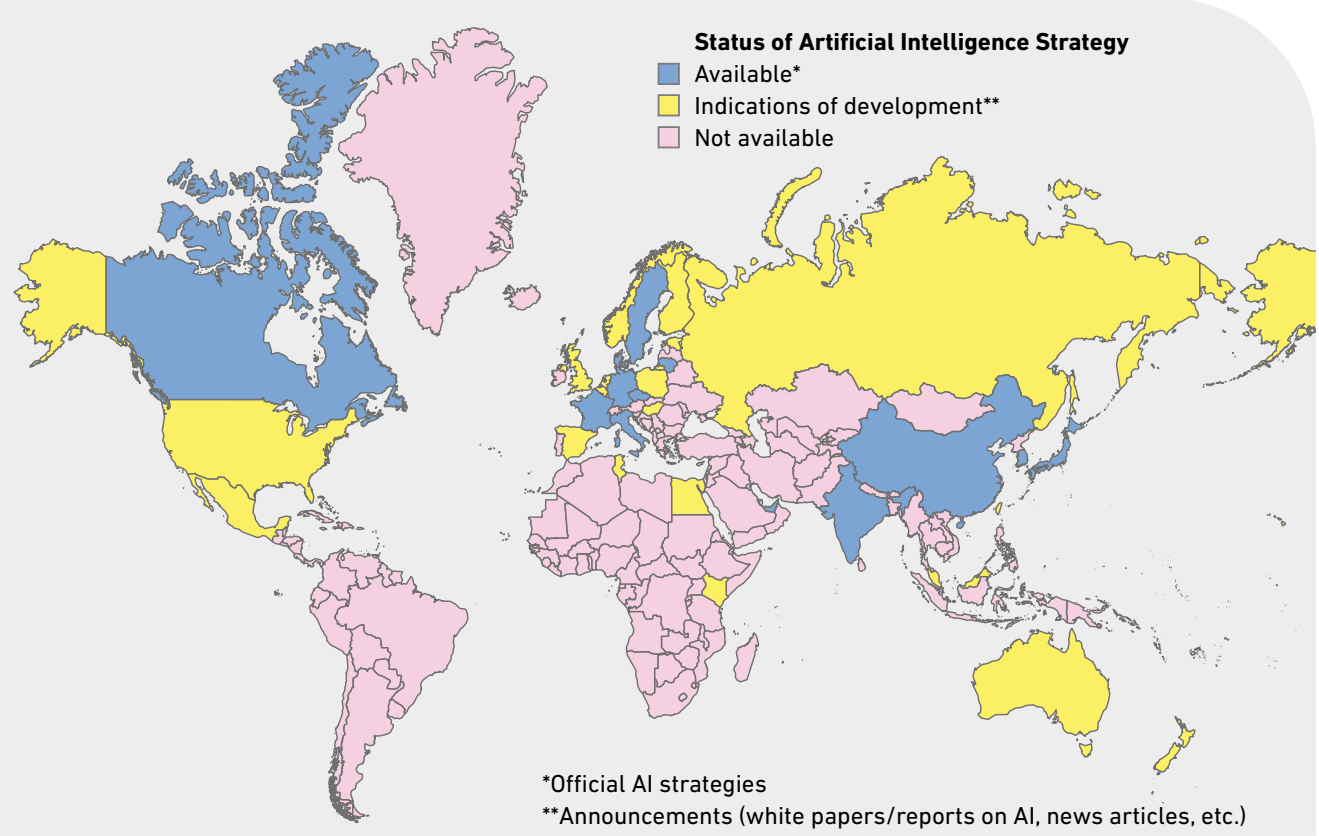
A growing number of national and international AI strategies and reports reflect the strategic importance of AI in the domain of security, health, finance, and public services. According to DiploFoundation's comparison of national AI strategies, a total of 13 countries have published official AI strategies. Media announcements and official documents (e.g. white papers) indicate that another 20 countries following suit.

## The main goals: leadership and economic prosperity

In their respective documents, governments outline their objectives for development and implementation, and ways of mitigating AI's potential negative impact on employment, societal inequalities, and the wellbeing of society.

The Chinese strategy, published in 2017, sets out three fundamental goals: (a) reach a level of AI development that is comparable with globally advanced levels by 2020; (b) achieve major breakthroughs in basic theories of AI by 2025; and (c) be a world leader in AI theories, technologies, and applications by 2030.

Leadership also features in the German strategy that wants to secure 'Artificial intelligence made in Germany' as a 'globally recognized quality mark'. Ten of the official national AI strategies explicitly cite leadership aspirations.



Economic prosperity resulting from advances in AI is also an objective. South Korea highlights that intelligent IT should generate a revenue amounting to KRW 460 trillion (~ €340 billion) by 2030, while China estimates that 26% of its GDP by that same year will be derived from AI-related activities. In a similar fashion, India's strategy '#AIforall' expects AI to contribute to an increase in its annual growth rate by 1.3% by 2035.

### Data in national AI strategies

The high relevance of data for AI is reflected in nearly all AI official strategies. Its availability is seen as the driving force behind AI development.

While some countries acknowledge the availability of large quantities of quality data sets, others, including Denmark and Japan, highlight the need for access to and digitalisation of publicly held data so as to develop AI-related capacities. To this end, the Villani Report, which served as the basis for France's AI strategy, calls for the development of new means of sharing, governing, and producing data. It also emphasises that a 'firm stance on data transfer outside the European Union' has to be ensured given that data is an issue of sovereignty.

The UN also identifies robust, open, inclusive, and representative data sets as one of the key areas for action given that AI is perceived as an opportunity for achieving the SDGs.

### Other themes tackled by national AI strategies

One of the recurring themes in national AI strategies and reports is AI research and development given that it appears in 12 documents. Lithuania and Canada both emphasise the importance of collaboration, incentives for investment, as well as talent retention/development, which among other things entails reskilling and is often discussed on the subject of future of work. In fact, it was addressed in ten of the official strategies. A number of strategies underlined that technologies including AI do not increase unemployment but cause shifts in labour.

AI is not regarded as an objective or as an end in itself but rather as a tool at the service of the public and society that can be used to pursue economic, commercial, and public interests. To this end, 11 out of 14 official documents address ethics-encompassing issues such as the responsible use of AI, and respect for privacy, transparency, and equality.

**Top 5 themes in official AI strategies**

| Theme | National strategies |
|---|---|
| Data |  |
| Research and development |  |
| Future of work |  |
| Ethics |  |
| Leadership |  |

# Policy discussions in Geneva

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

## *33rd Forum of the UN Centre for Trade Facilitation and E-Business (UN/CEFACT)* – 1–5 April 2019

The forum focused on how digital technology can help achieve the goals set out in Agenda 2030. Experts and delegates from 34 countries discussed projects in support of cross-border exchange of information. A more inclusive system for exchange of information would help developing countries and smaller businesses participate in global trade. Standards and a more innovative approach to e-services could lower the barriers for micro, small, and medium-sized enterprises in accessing global trade.

## *UNCTAD eCommerce Week* – 1–5 April 2019

The conference focused on the theme 'From Digitalization to Development', and addressed three main topics: E-commerce and digital business models, regulatory frameworks, and emerging technologies. Some sessions explored measures to foster inclusion in the digital economy, such as incentives to small and medium enterprises (SMEs), and developing frameworks which better facilitate the cross-border flows of data, services, and goods. Regulatory frameworks-related sessions focused on the current e-commerce negotiations at the World Trade Organization (WTO) and reflected the polarised divisions among member countries. Discussions on emerging technologies focused on issues related to blockchain technologies, artificial intelligence (AI), and machine learning.

*Read our reports from the sessions.*

## *WSIS Forum 2019* – 8–12 April 2019

The forum looked at the role of ICTs in achieving the sustainable development goals (SDGs). It also highlighted the links between digital technology and SDG priority areas, including health, hunger, accessibility, education, youth inclusion, employment, gender empowerment, the environment, infrastructure, and innovation. The high-level policy sessions emphasised narrowing the digital divide, and fostering inclusiveness through ICTs.

*Read our reports from the sessions.*

## *ILO100 - Law for Social Justice* – 15–17 April

The International Labour Organization's three-day conference, which marks the ILO's 100th anniversary, focused on law for social justice. The conference underlined the ILO's work in shaping international law in the field of social and labour rights, and reflected on current and future ILO standard-setting efforts in the broader scenario of the human rights agenda, and the normative context of international organisations. Speakers from the International Court of Justice, the International Law Commission, as well as leading scholars and practitioners, discussed four main themes: philosophy of law, human rights, public international law, and the law of international organisations.

# The main global digital policy events in May

**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.**

May

### 7–8 MAY
**5th SEEDIG Annual Meeting (Bucharest, Romania)**

The 5th South Eastern European Dialogue (SEEDIG) Annual Meeting will focus on topics which are relevant for the region, such as the digital divide, cybersecurity, Internationalised Domain Names (IDNs), digital rights, and the digital economy.

### 13–17 MAY
**22nd Session of the Commission on Science and Technology for Development – CSTD (Geneva, Switzerland)**

The 22nd session of the CSTD will discuss the Commission's two priority themes for 2019: the impact of rapid technological change on sustainable development, and the role of science, technology, and innovation (STI) in building resilient communities.

### 15 MAY
**G7 Tech for Humanity (Paris, France)**

An informal meeting of Digital Ministers of G7 countries, 'Tech for Humanity' will cover three main themes: combating online hate speech; developing AI technologies and their contribution to combating inequality; discussing the G7 strategy at the rise of the data economy and the need to build trust in digital technologies. This event will take place in parallel to the Tech for Good Summit, also in Paris on 15 May.

### 15 MAY
**Christchurch Summit (Paris, France)**

The summit, organised and co-chaired by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron, aims to see countries and tech companies commit to the 'Christchurch Call', a pledge to eliminate terrorist and violent extremist content online.

### 20–24 MAY
**RIPE78 (Reykjavik, Iceland)**

The meeting will bring together Internet service providers, network operators, and other stakeholders, to discuss various topics: IPv6 deployment, managing IPv4 scarcity, data centre technologies, network and Domain Name System (DNS) operations, Internet governance and regulatory practices, network and routing security, content delivery, Internet peering and mobile data exchange, and connected Things (Internet of Things – [IoT]).

### 28–30 MAY
**International Conference on Cyber Conflict (CyCon) 2019 (Tallinn, Estonia)**

Under the main topic of 'Silent Battle', the 11th CyCon will focus on cyber threats to democracies and how to address this challenge to national security from a strategic perspective. Various sub topics will be explored, including vulnerabilities, exploits, and patches; detection and attribution; responsibility; and situational awareness.

### 28–31 MAY
**AI for Good Global Summit 2019 (Geneva, Switzerland)**

Hosted by the ITU in partnership with UN sister agencies, XPRIZE Foundation and ACM under the theme 'Accelerating progress towards the Sustainable Development Goals (SDGs)', the Summit connects AI innovators with problem owners; identifies practical AI applications to accelerate progress towards the UN SDGs; and ensures trustworthy, safe, and inclusive development of AI technologies and fair access to their benefits.

June

# On the observatory: Tools for following digital policy

**Digital policy is complex, and moves at a fast pace. The GIP's *Digital Watch* observatory has a range of tools to help practitioners keep in step, tools that systematise global digital policy discussions, events, and forums.**

First developed in 1997, the **taxonomy of digital policy** is regularly reviewed to account for emerging trends and new developments. The GIP *Digital Watch* observatory currently features over 40 digital policy areas, classified under seven broad clusters, or baskets: Infrastructure, Security, Human Rights, Legal, Economic, Development, and Sociocultural. Browse the taxonomy at dig.watch/issues

The observatory's **interactive calendar of digital policy events** shows past and future digital policy events according to the geo coordinates of the city they were or will be held in. Events can be filtered by name, title keywords, date, and digital policy issue they are concerned with. Browse the calendar at dig.watch/events

Geneva Internet Platform DigitalWatch

Missed the deadline to register for a conference? Forgot an important digital policy event? **DeadlineR** is a notification system that allows observatory users to receive e-mail reminders of policy event deadlines. By subscribing to these notifications, users receive e-mails with various deadlines associated with the event, such as event registration, workshop submission deadline, and start-date reminders. Visit the Upcoming Events section at dig.watch/events, choose your digital policy event, and click on 'Notify me about deadlines.'

Digital policy involves a wide variety of stakeholders, or actors. The **map of actors** lists the main actors alphabetically, with additional options of filtering by name, stakeholder group, region, and the policy areas they engage in. Actors can also be explored by their location on the world map. Browse the map at dig.watch/actors

The observatory is rich in resources, including reports from main digital policy events, instruments, publications, and other content. Resources, including developments in digital policy, can be located using the observatory's **smart search**. The initial search results can be further filtered by date, issue, and type, allowing for deeper layers of granularity by narrowing the search even more.

**About this issue**
Issue no. 39 of the *Digital Watch* newsletter, published on 14 May 2019, by the Geneva Internet Platform and DiploFoundation | Contributors: Cedric Amon, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Stefania Grottola, Marco Lotti, Nataša Perućica, Vladimir Radunović and Mili Semlani | Design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić, Diplo's CreativeLab. | More digital policy updates available on https://dig.watch

**Our new design**
Our newsletter has been redesigned! It's now bigger and better. We have added more in-depth articles, a new section on data analysis, and more visible timelines. We would love your feedback: digitalwatch@diplomacy.edu

**On the cover**
*5G geopolitics: A game of e-thrones.* Credit: Vladimir Veljasević (design), Patrick Borg (concept)
DiploFoundation (2019) https://creativecommons.org/licenses/by-nc-nd/4.0/

Geneva Internet Platform DigitalWatch

The Geneva Internet Platform is an initiative of:
Schweizerische Eidgenossenschaft, Confédération suisse, Confederazione Svizzera, Confederaziun svizra
Republique et Canton de Geneve
Université de Genève
ETH zürich
DiPLO www.diplomacy.edu