Geneva Internet Platform
DigitalWatch
NEWSLETTER

You receive hundreds of pieces of information on digital policy.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.

DIGITAL POLICY TRENDS IN MAY

1. RANSOMWARE ATTACKS ON THE INCREASE

The WannaCry ransomware cyber-attack, which hit thousands of systems around the world, raised concern over the span of the attack and the losses it generated. The software hit healthcare services – most notably the National Health Service (NHS) which it crippled for hours – government departments, schools, and many businesses worldwide. Within hours of the first reports on 12 May, the software spread to more than 100 countries.

Who was behind the attack, and who were the first responders? In our just-in-time webinar on WannaCry, we looked at the countries' responses to the attack, and the use of cryptocurrency to amass the funds. Although Microsoft had issued a patch for its software as soon as the vulnerability was leaked, governments had the responsibility to report to companies any vulnerabilities they exposed.

The general patch-and-pray approach by many companies meant that not enough attention was put into ensuring their products were safe. Users are just as responsible to ensure they keep their systems updated. Following the attack, Microsoft reiterated its call for a Digital Geneva Convention. Could this Convention stop such an attack? Probably not. The very Internet architecture opens the space for such attacks. However, the convention could improve coordination between governments and other players, and increase the chance of identifying criminals.

As for the economic implications, it is now clear that the ransom generated was considerably low. Why was this, and what other losses were generated? *Turn to page 6 for more analysis.*

2. COURT DECISION EXPECTED TO IMPACT THE FUTURE OF THE SHARING ECONOMY

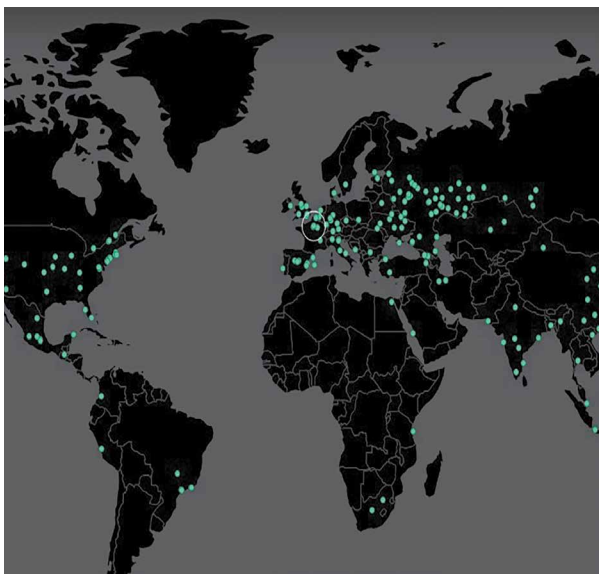
This month, we inched closer to a decision on whether Uber is an information society company, or a transport company – a question that is being considered by the Court of Justice of the European Union (CJEU). Although a ruling has not been yet made, on 11 May the Advocate General gave his opinion on the matter, stating that Uber is a transport company.

The service offered by Uber cannot be classified as an information society service, as the service amounts to a comprehensive system for on-demand urban transport.

As such, Uber should be subject to the conditions under which non-resident carriers operate transport services within EU member states, with implications for taxi drivers and the benefits they would be entitled to as employees.

If the court confirms the opinion, the landscape for the whole sharing economy will be severely impacted.

Continued on page 3



The scale of the WannaCry ransomware cyber-attack was unprecedented. The number of countries hit, and the damage it caused were extensive. Can the same be said for the ransom it generated? *More on page 6.*

IN THIS ISSUE

Issue no. 21 of the *Geneva Digital Watch* newsletter, published on 30 May 2017, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Stephanie Borg Psaila, Jovan Kurbalija, Virginia (Ginger) Paque, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, layout by Aleksandar Nedeljkov, Diplo's CreativeLab | In addition to the newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (http://dig.watch) and join discussions on the last Tuesday of every month online, at local hubs, or at the GIP (http://dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu

GENEVA DIGITAL DEVELOPMENTS

CSTD Working Group on Enhanced Cooperation: 3rd meeting

The main discussion during the Group's third meeting, held on 3–5 May, focused on the future architecture of global Internet governance. Two main views were prevalent: on the one hand, most developed countries and industry representatives believe that all Internet governance issues are being adequately dealt with by the existing mechanisms that use multistakeholder processes; on the other hand, some civil society actors and many developing countries argue that the establishment of a UN-based mechanism would facilitate enhanced co-operation in digital matters. The proposed compromise solutions have not gathered significant support yet. *Read the event report.*

The Media's Role in Advancing Peaceful, Just and Inclusive Societies

The discussion, organised on 3 May by the Permanent Mission of Greece to the United Nations Office and the UNESCO Geneva Liaison Office, focused on justice for all as a prerequisite for freedom of expression and sustainable development, freedom of expression and freedom of information in fostering more inclusive societies, and safety of journalists and media freedom as a means of ensuring public access to information. Participants also discussed the role of digital technologies as disruptors of the traditional media environment, and underlined the challenges brought to freedom of expression by the so-called 'private censorship' imposed by online intermediaries. Despite the transformative effect of digital technologies, there will always be 'an intricate relationship between press freedom, freedom of expression, accountability, social justice, and human dignity'. *Read the event report.*

Commission on Science and Technology for Development, 20th Session

At its 20th session, held on 8–12 May, the Commission addressed two priority themes: new innovation approaches to support the implementation of the Sustainable Development Goals (SDGs), and the role of science, technology, and innovation in ensuring food security by 2030. The five-day meeting resulted in the adoption of two draft resolutions to be presented to the Economic and Social Council: the first includes several recommendations for governments to support science, technology, and innovation efforts that foster the global expansion of ICT infrastructure, products, and services, including broadband Internet access to all people; the second underlines the need to close the digital divide, and the value of multistakeholder co-operation and engagement in Internet governance processes, among others. *Read the event report.*

GIS for a Sustainable World Conference

The conference, held on 9–11 May, was dedicated to exploring modalities in which Geographic Information Systems (GIS) and innovative solutions like drones and virtual and augmented reality applications can unlock the full potential of data and contribute to achieving the SDGs. Participants underlined the need for capacity-building and know-how by the public authorities to develop GIS-based projects that make use of big data. Debates also revolved around new types of web and cloud-based GIS applications and how they can enhance collaboration and data sharing across organisations and communities. As GIS applications involve the use of data, the question of data protection was also raised during the event, and participants acknowledged the fact that data sharing and use requires trust-building. *Read the event report.*

WSIS Forum 2017 Open Consultation Process: Final Brief

The final brief, held on 10 May, outlined the preparations for the upcoming World Summit on Information Society (WSIS) Forum, which will include a full week of high-level sessions, workshops and innovative events, including a photo contest, a hackathon and a TED Talk. The brief also detailed logistical aspects, such as the premises, the registration process, and online participation opportunities. More than 2000 people are expected to attend the annual stock-taking event of the WSIS on 12-16 June. This year's theme will address 'Information and Knowledge Societies for SDGs'. The GIP will report from the event.

Open Geneva Hackathons

The festival of independent hackathons took place on 12–14 May, as part of the digital strategy of the University of Geneva, and was aimed at promoting and encouraging open innovation generated by citizens, associations, and institutions. The three-day event brought together about 400 participants who, in the framework of more than 20 hackathons held all over Geneva, developed practical solutions in areas such as smart cities, gender equality, programming for kids and parents, 3D/virtual reality for bioinformatics, open libraries, cryptocurrencies and blockchain technologies, human rights and responsibilities, and embedding SDGs into human practice.

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

DIGITAL POLICY TRENDS IN MAY

Continued from page 1

Uber might not have major difficulties adapting to the ruling, considering it generates $6.5 billion in revenue and $2.8 billion in net income. The same cannot be said about the company of a few years ago however; it is questionable whether it would have succeeded in that kind of regulatory environment when it had just started off.

The judgment would impact the future of the sharing economy, not only in Europe but also on other continents. The CJEU is expected to deliver its judgment in the coming weeks.

Uber has been involved in legal action in 25+ countries. View the interactive database for details.

3. NET NEUTRALITY: ANOTHER U-TURN?

The 2015 Open Internet order, adopted by the US Federal Communications Commission (FCC), took another hit this month after the FCC, led by newly appointed chairman Ajit Pai, voted to start a process that would roll back the net neutrality rules, which request equal treatment for Internet traffic.

The vote means that the proposal to overturn the classification of broadband providers as utility carriers, put forward in April by Pai, is now an official FCC proposal and is open for public comment until August. The proposal also envisions the repealing of the 'general conduct rule' that allows the Commission to investigate business models of Internet providers that might be uncompetitive.

Although Pai has previously said that he favours an open Internet, it remains to be seen what will happen with the 2015 net neutrality rules. Many Internet providers believe that the rules discourage them from investing in the infrastructure to provide a faster and better service. However, Democratic FCC Commissioner Mignon Clyburn, who voted against the plan, and many net neutrality proponents believe that this will jeopardise 'the ability of the open internet to function tomorrow, as it does today'.

4. MORE BILATERAL TAX SETTLEMENTS RECORDED

Bilateral settlement of tax disputes has become common occurrence. This month, Alphabet, Google's parent company, settled a year-long tax-dispute with Italy, agreeing to pay €306 million for the period 2002–2015.

Alphabet has already settled similar disputes with British authorities, and is still negotiating tax settlements with France and Spain. Moreover, a few months ago, Facebook paid £4.2 million to the British tax authorities, a great increase from the £4,327 paid in 2014, which had caused a stir for being so low.

Bilateral tax settlements are used as a corrective measure for lack of taxation rules for new Internet business models. Internet companies also accept it as a way to address criticism that they do not contribute to social well-being. So far, the contribution of the Internet industry to providing social stability and cohesion has been limited. According to a study by the US Public Interest Research Group, the top 30 US tax-withholding companies include 10 major Internet companies.

Given current fiscal difficulties, one can expect further pressure on the Internet companies to pay taxes in the jurisdiction where they gain a profit, even if they are not formally obliged to do it due to the lack of rules for taxation of Internet activities. An Italian court, for example, maintains that Amazon has evaded around €130 million in taxes in Italy.

Following examples of the EU member states, other countries are likely to similarly pursue taxes from multinational Internet companies.

5. DATA PROTECTION AUTHORITIES SANCTION FACEBOOK OVER PRIVACY BREACHES

In May, Facebook was fined €150 000 by the Commission Nationale de l'Informatique et des Libertés (CNIL), France's data protection watchdog, for violating data protection rules.

The company failed to explain to its users how personal data is tracked, and unlawfully tracked users' browsing activity'. The company's policies and practices are under investigation in four other European countries.

The Belgian Privacy Commission believes the company is breaching both Belgian and EU data protection laws through its tracking practices. The Dutch and Spanish Data Protection Authorities have also concluded that Facebook is breaching local law, and are now taking further action. The question of jurisdiction, raised in the course of a complaint by a German Data Protection Authority, is being tackled by the CJEU.

In each of these investigations, the company argued that the applicable data protection law was the Irish law. The authorities however argue that their respective national data protection law applies to the processing of personal data of users in their countries.

While Facebook and the authorities await the courts' rulings, the EU General Data Protection Regulation (GDPR), which will come into effect in May 2018, is expected to strengthen the role of European data authorities. The GDPR will also ensure that the same data protection rules are applied uniformly within the EU. *Are you GDPR-ready? Turn to page 8 to test your knowledge.*

Pro-net neutrality activists gather at the FCC headquarters, Washington, on 15 May. *Credit: John Shinkle/POLITICO*

DIGITAL POLICY: DEVELOPMENTS IN MAY

Global IG architecture

same relevance

Microsoft CEO Brad Smith has renewed the call for a Digital Geneva Convention in response to the WannaCry ransomware cyber-attack. Among the proposed provisions of the convention is the requirement for governments to report vulnerabilities to vendors.

The UK's Conservative Party plans to considerably increase Internet regulation, and to force Internet companies to abide by new rules to ensure a safer online environment. 'While we cannot create this framework alone, it is for government, not private companies, to protect the security of people and ensure the fairness of the rules by which people and businesses abide. *More on page 7.*

The G7 has put pressure on Internet companies and Internet service providers to increase their efforts to remove extremist content.

Sustainable development

same relevance

The second Multistakeholder Forum on Science, Technology and Innovation (STI) for the SDGs (15–16 May, New York) considered ways STI can contribute to realising six of the SDGs, including goal 9 (industry, innovation and infrastructure). During the High-level Event on SDG Innovation (17 May), technologists from Silicon Valley presented ideas for achieving the SDGs, and urged UN member states to foster a culture of risk-taking.

Security

increasing relevance

The WannaCry ransomware cyber-attack, considered to be the biggest ransomware outbreak detected so far, infected thousands of devices worldwide. The malicious software encrypted data on the infected devices and demanded a ransom of $300 in bitcoins in order to release the data.

The US President has signed a cybersecurity executive order aimed at strengthening the security of federal government institutions. Measures include moving government services to the cloud, and implementing a set of best practices in cybersecurity developed by the National Institute of Standards and Technology, known as the NIST Framework.

Microsoft's latest policy paper, *Cybersecurity Policy for the Internet of Things*, notes that securing the IoT is an urgent matter that requires collaboration across borders, sectors, and organisations.

At the G7 summit in Taormina, G7 leaders emphasised their 'commitment to increased international cooperation to protect an accessible, open, interoperable, reliable and secure cyberspace', and agreed to work together and with other partners to address cyber-attacks and mitigate their impact on critical infrastructures.

E-commerce & Internet economy

increasing relevance

The Advocate General of the CJEU has opined that Uber should be classified as a transportation service. *More on page 3.*

Alphabet, Google's parent company, has agreed to pay €306 million to settle a year-long tax dispute with the Italian government for the period 2002–2015. *More on page 3.*

In a report on a European agenda for the collaborative economy, the Internal Market and Consumer Protection Committee of the European Parliament has invited the European Commission and EU member states to address regulatory grey areas. The report recommends that any regulation should avoid restricting the collaborative economy.

Digital rights

increasing relevance

The European Commission (EC) has fined Facebook €110 million for giving misleading or incorrect information during the EC's 2014 vetting of its deal to acquire the messaging service WhatsApp. The Commission Nationale de l'Informatique et des Libertés (CNIL), France's data protection watchdog, has fined Facebook €150 000 for violating French data protection rules. *More on page 3.*

Turkey has blocked Wikipedia after passing a law that bans access to websites that are considered obscene or a threat to national security. China will launch an online encyclopaedia, in 2018, with content created by thousands of scholars from state-run universities.

A new parliamentary report by the UK Home Affairs Select Committee has found that social media companies are 'shamefully far' from tackling illegal content. The firms are 'big enough, rich enough and clever enough' to solve the problem, yet it takes too long for illegal and dangerous content to be removed.

Jurisdiction & legal issues

same relevance

A Viennese Court of Appeals has ruled that Facebook must remove posts deemed to be hate speech. Merely blocking the posts in Austria will not be enough: Facebook must delete the posts across the platform. The company is expected to appeal.

The European Parliament has voted in favour of new data portability rules that will enable users to enjoy services they are subscribed to even when they travel to other countries in the EU. As of 2018, users will not have to pay extra to watch series, music, or sports events that are subscribed to in their country, when travelling.

Infrastructure

same relevance

The Empowered Community (EC) created within the Internet Corporation for Assigned Names and Numbers (ICANN) as a consequence of the Internet Assigned Numbers Authority (IANA) stewardship transition, will undergo its first test. Following approval by the ICANN Board of amendments to the organisation's Fundamental Bylaws, the EC is now called to consider and approve these amendments before they can go into effect.

The European Commission has launched a public consultation on the evaluation and revision of the Regulations for .eu, the country code top-level domain (TLD) for the EU. EURid, the registry for .eu and .ею has announced that the World Intellectual Property Organisation (WIPO) will become an alternative dispute resolution provider for the two TLDs starting June.

The RIPE Network Coordination Centre (RIPE NCC), the regional Internet registry (RIR) for Europe, the Middle East, and parts of Central Asia, has launched a programme aimed to assist governments with their IPv6 allocation requests. The aim of the programme is to help governments accurately calculate the amount of addresses that they need.

Net neutrality

increasing relevance

The US FCC has voted to start a process that could lead to a roll back of the net neutrality rules it had adopted in 2015. *More on page 3.*

Meanwhile, the US Court of Appeals for the District of Columbia Circuit has upheld the FCC's net neutrality rules in a case brought against the rules by representatives of the US broadband industry. The court affirmed that the FCC had ample authority to reclassify ISPs as common carriers, and dismissed the argument that the FCC's policy infringes upon the free speech rights of broadband companies.

New technologies (IoT, AI, etc.)

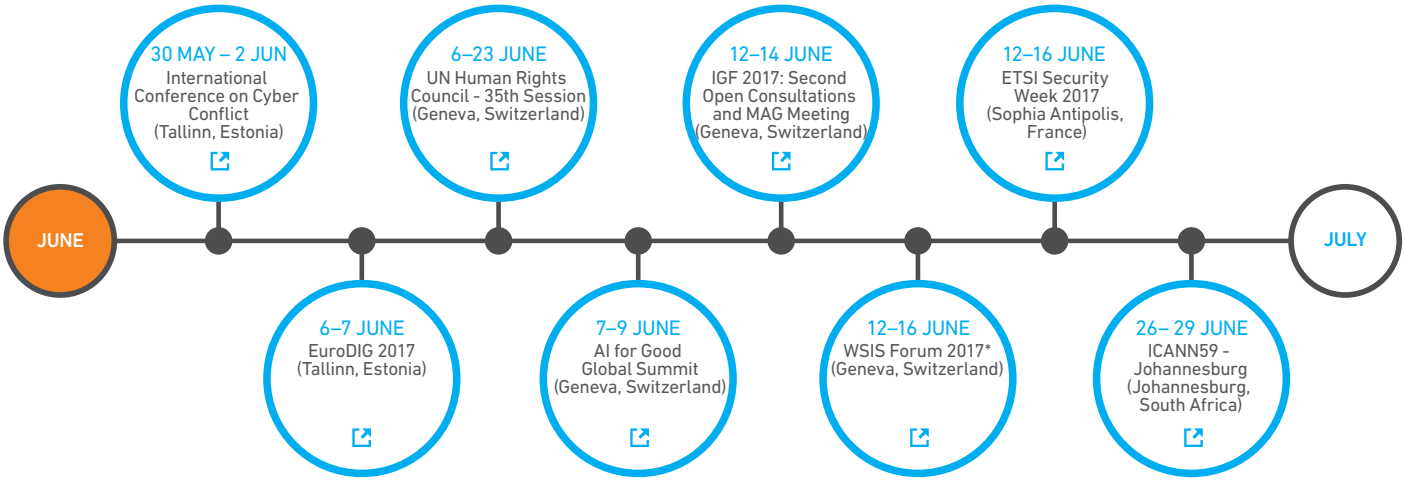
same relevance

Researchers have discovered a new Internet of Things (IoT) botnet, called Persirai, which targets over 1 000 camera models. Around 120 000 cameras are vulnerable; users may not be aware that their cameras are exposed.

The Partnership on Artificial Intelligence, founded in September 2016 by Amazon, DeepMind/Google, Facebook, IBM, and Microsoft, with the aim of developing guidelines for best practices, has announced an expansion with new partners, as well as the launch of a series of initiatives. New initiatives include the creation of topic-specific and sector-specific working groups to research and formulate suggestions for best practices, and the creation of a Civil Society Fellowship programme aimed at assisting non-profits and NGOs to collaborate on topics in AI and society.

An Australian parliamentary committee has called for stronger regulations for drones, in three areas: safety awareness and training for users, registration and tracking of drones, and the introduction of geofencing technology and drone shields.

AHEAD IN JUNE



*The GIP will report from the WSIS Forum 2017. Visit our dedicated page for session reports, updates, and a summary report. For more information on upcoming events, visit http://dig.watch/events

IS CYBERSECURITY COUNTER-INTUITIVE?

The WannaCry ransomware cyber-attack this month captured the global media attention. The scale of the ransomware was unprecedented. The number of countries hit, and the damage it caused were extensive. Can the same be said for the ransom it generated?

The aim of a ransomware cyber-attack, as the name suggests, is to extort the victim into paying money in order to regain access to their data. In recent years, there has been a shift in ransomware targets: in search for larger financial gains, perpetrators have turned from individuals to businesses. In fact, according to researchers at Kaspersky, attacks on businesses increased threefold in 2016, compared to a twofold rate of increase in attacks on individuals.

The WannaCry attack targeted everyone: businesses, government departments, hospitals, schools, and individuals. Similar to other malicious software, WannaCry encrypted data on the device and demanded a ransom of $300 to be paid to a given Bitcoin wallet within three days, or $600 within seven days. Three Bitcoin wallets were tied to WannaCry.

Within a space of two weeks following the attack, it became clear that WannaCry did not generate a high ransom. By 11:00 CEST (27 May 2017), the three Bitcoin wallets tied to the ransomware received 335 payments totalling 50.5 bitcoins ($106 050). Many expected that the ransom would be higher, considering the scale of the attack.

There are several possible explanations:

- Victims may have had archives with backed-up data;
- Victims may have paid a ransom using a different currency;
- Victims may not have known what to do, and how to do it;
- An unidentified organisation could have paid, even negotiated, a bulk ransom payment;
- Victims could have managed to unlock their data, bypassing the malicious software;
- The perpetrators may have been successfully stopped in their tracks, and the malicious software defeated, by the international cybersecurity community;
- The motive might not have been the ransom but to put systems down, causing an effect similar to a DDoS attack, without the need for a botnet.

Most likely, it is a combination of the above. Tools for recalling decryption keys were quickly developed. Although breaking an encryption is a difficult feat, the process of creating keys and encrypting data involves mathematical operations conducted on a computer using Windows services which can leave work traces logged in computer memory. In computer science, breaking an encryption is more about exploiting imperfections than about algorithms and mathematics. For instance, snooping on WhatsApp is generally carried out through keyloggers that capture keyboard strokes, rather than by breaking the application's encryption.

Procedures for computer back-ups are usually integrated within standards and good practices; this is often the case in developed countries where a systemic approach is usually adopted. The most likely reason why the UK National Health Service's (NHS) systems were endangered was not about the loss of data, but the time required to restore the system, which led to the suspension of a number of operations. In addition, IT support was able to react faster on systems which run on more up-to-date software – a scenario that is more prevalent in developed countries.

Unlike other viruses, WannaCry propagated through the network and infected computers like a worm. Users of infected computers, therefore, did not have to activate the infected file or link for the software to continue spreading. As a result, the malicious software propagated widely, infecting many more computers than any previous ransomware. The ability to restore data from back-ups, however, bypasses the need to pay ransom. A higher number of infected computers therefore, does not automatically mean a higher number of ransom being paid.

Despite the low figures, the collateral damage was still extensive. Losses extended beyond the amount of the ransom, and included:

- major disruptions in systems, and in the case of healthcare facilities, placing lives in jeopardy;
- financial losses from the disruption to business operations;
- financial losses incurred to restore the systems and files;
- temporary or permanent loss of sensitive or proprietary information;
- potential harm to reputation.

One of the undeniable outcomes of the attack is increased cybersecurity awareness. Both end-users and organisations will surely focus more on cybersecurity matters. Although not among the most dangerous attacks we have seen so far, its effects have also helped raise awareness of cybersecurity as a geopolitical issue.

However, cybersecurity actions can lose their credibility if they focus too much on hype and too little on the facts – and making them known. Cybersecurity relies heavily on the availability of information. The more cybersecurity is intuitive for people, the safer the online world can be.

Learn more about the attack and the technology behind it on the GIP Digital Watch observatory. Read the digest and view the recording of the GIP's just-in-time webinar, from 18 May.

Which countries were attacked by the WannaCry ransomware? View our interactive map with details on each country hit.

THE ROLE OF DIGITAL POLICY IN CAMPAIGNS AND ELECTIONS

Digital policy issues have become central in elections worldwide. This month, digital issues were prominent in European electoral campaigns. How is digital used in campaigns, and what does it represent?

In electoral campaigns, digital is typically framed in the narratives of both hope and fear. Technology presents new opportunities for education, health, and commerce. Digital growth is transforming industries and is giving economies a hope for further growth across every sector.

Digital technology also presents several risks, from cyber-attacks and cyber conflicts, to increasing inequalities and fragmentation. The risks can lead to breaches of human rights, economical losses, and damage to infrastructure.

In France, the presidential elections resulted in the victory of Emmanuel Macron, who is keen on technology, and is a strong supporter of the start-up technology industry in France. His embrace of technology and modest deregulation was described by his critics as the 'Uberisation of society', referring to the upheavals that innovation and digital transformation – which he believes in – may bring. Throughout his campaign, he referred to digital technology and policy as a way of energising the French economy, and showed support for the EU Digital Single Market.

Yet, he sees tech companies playing a more co-operative role in the fight against terrorism. 'Governments, as long as they are democratic, should be able to access terrorist content on social networks and instant messaging services. We need to figure out the terms and the safeguards. But the goal is clear.' It remains to be seen how he can use the digital angle as way of reforming French economy and society.

Digital policy also plays an important role in the UK election campaign. Prime Minister Theresa May, announced new investment for emerging technologies, during her term in office in 2017. New technologies, in fact, featured prominently in the green paper on industrial strategy, launched earlier this year.

However, the risks emanating from cybercrime, cyber-attacks, and the spread of violent online extremism, represent a major concern for the Conservative Party, whose ambition according to its electoral manifesto is to make Britain 'the global leader in the regulation of the use of personal data and the Internet'.

In response to the Manchester Arena attack, May said that she believes that more can be done – especially by technology companies – to tackle the threat posed by extremist content online.

This echoes the party's manifesto. In a major departure from UK foreign digital policy, which traditionally opposed the adoption of international conventions, the Conservative Party is clear: 'We will open discussions with the leading tech companies and other like-minded democracies about the global rules of the digital economy, to develop an international legal framework that we have for so long benefited from in other areas like banking and trade. We recognise the complexity of this task and that this will be the beginning of a process, but it is a task which we believe is necessary and which we intend to lead.'

In Malta, emerging technologies including the Internet of Things, Artificial Intelligence, blockchain technology, big data analytics, and wearable technology, are the focus of the main two parties contesting general elections on 3 June. Currently holding the Presidency of the Council, Malta has always embraced global technological developments as a way of overcoming challenges unique to its small size.

Digital technology is also affecting the elections themselves. Fake news has been in focus since the US presidential election in November, and is driving technology companies to forcefully tackle the issue, amid criticism over their roles and responsibilities. Specific aspects related to elections, such as the use of social media, data-mining, and e-voting and e-counting, are also having their fair share of attention.

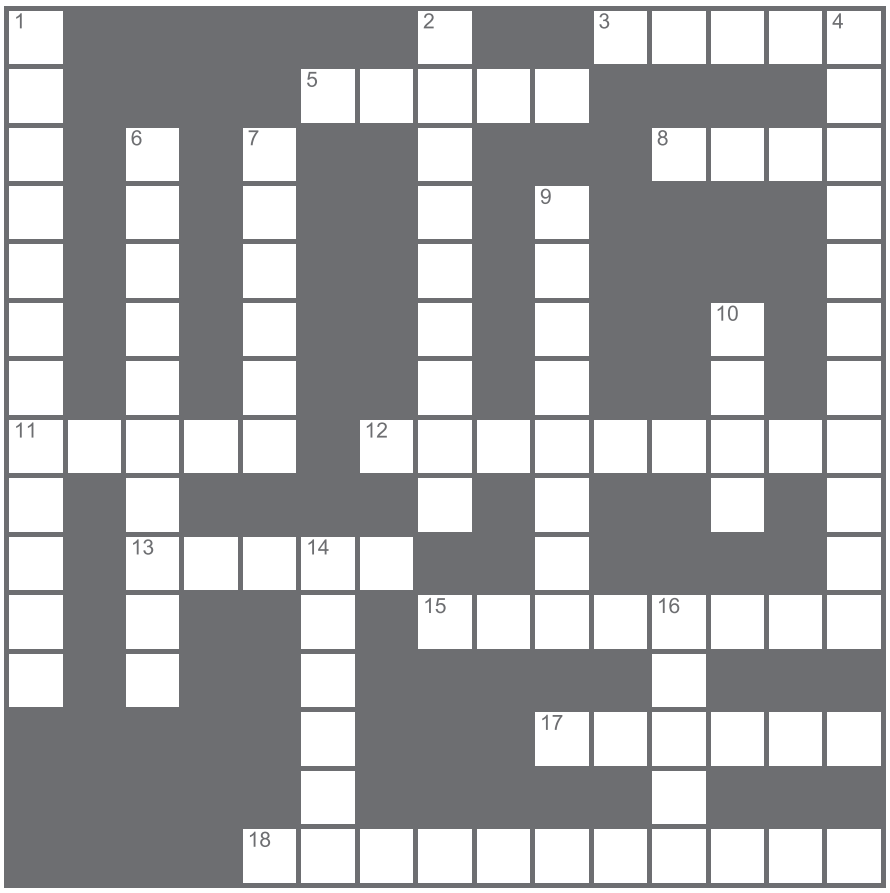
Coming up in the autumn, the German elections will offer another occasion to revisit digital policy proposals put forward by one of Europe's leading digital economies.

Present at the G7 Summit in Taormina, on 26-27 May, UK Prime Minister Theresa May joined other leaders in demanding Internet intermediaries to more actively fight online extremism. *Credit: Justin Tallis / AFP*

GENERAL DATA PROTECTION REGULATION: ARE YOU READY?

The European Commission's new legislation on data protection, the General Data Protection Regulation (GDPR), will impact the way data is handled in the EU and beyond. Given the centrality of data flows for the modern world, it will affect the global digital economy and politics.

The GDPR comes into effect a year from now – on 25 May 2018. Are you acquainted with the concepts? Is your organisation prepared? Test your knowledge and preparedness with our crossword, and learn more about the GDPR.



Across

3 Data plays a central role in the 4th industrial revolution. The global forum in which the 4th industrial revolution was discussed prominently is hosted in this Swiss city. (5)

5 The GDPR was approved by the European Parliament on 14 _____ 2016 and will become applicable in May 2018. (5)

8 The acronym of a controversial transatlantic agreement which contained norms against data localisation. This agreement was put on the backburner by the current US administration. (4)

11 Digital data is largely stored in server farms, known as the _____. (5)

12 An individual is said to be _____ if he/she cannot be identified. (9)

13 The protection afforded by the GDPR applies to natural persons; it does not cover data concerning _____ persons. (5)

15 The name of the recent ransomware attack which prevented users from accessing data on their computers unless they paid the ransom. (8)

17 According to the GDPR, the architecture of applications should take data protection into account when being developed. This is referred to as data protection by _____ (6)

18 An engaging way of presenting information or data in an easy-to-understand graphical format. (11)

Down

1 _____ refers to the authority of the court and state organs to decide on legal cases. (12)

2 The GDPR introduces strict provisions on _____, which is the collection and analysis of personal data to gain insight into an individual's personality, behaviour, and habits. (9)

4 The lead _____ authority is the main data protection regulator which will supervise the cross-border processing activities of an organisation. (11)

6 The _____ is the individual or entity which determines the purposes and means of the processing of personal data. (10)

7 The Privacy _____ framework, which replaced the Safe Harbor, imposes stronger obligations on US companies to protect the personal data of EU citizens. (6)

9 The proposal to keep EU's data within Europe was named after a European city as the _____ cloud. (8)

10 Cross-border data _____ refers to the transfer of information or data beyond a country's borders. (4)

14 The name of a US company which pioneered the storing of data in the cloud, and which is still one of the top providers of cloud services globally. (6)

16 The last name of the Vice President of the European Commission who is leading the Digital Single Market process. (5)

Across: **3** Davos, **5** April, **8** TTIP, **11** Cloud, **12** Anonymous, **13** Legal, **15** WannaCry, **17** Design, **18** Infographic.
Down: **1** Jurisdiction, **2** Profiling, **4** Supervisory, **6** Controller, **7** Shield, **9** Schengen, **10** Flow, **14** Amazon, **16** Ansip.