DiPLO Policy Papers and Briefs – 9, 2018

A TIPPING POINT FOR THE INTERNET: PREDICTIONS FOR 2018

Jovan Kurbalija

Summary

- The year 2018 represents a tipping point for the Internet and its governance. Processes that have been evolving are now starting to mature. Policy decisions are needed. 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).

- Geopolitical shifts, in particular, will affect how the Internet is governed. The Internet is vulnerable to the fragmentation of global society, which is likely to accelerate in response to the ongoing crisis of multilateralism, as it depends heavily on multilateral rules and standards dealing with telecommunications, trade, and finances. If this crisis leads to further restrictions in the movement of people, capital, and goods across national borders, the same is likely to happen with the digital economy, including the cross-border flow of data and services.

- The first sign of a crisis in multilateralism in digital policy was the failure of the 5th UN Group of Governmental Experts (UN GGE) to reach consensus on a final report. Towards the end of 2017, the World Trade Organization (WTO) failed to agree on any mandate for e-commerce negotiations during the WTO Ministerial meeting in Buenos Aires.

- Given the crisis of multilateralism, it will be all the more important to use divergence in order to create convergence. While interests in digital policy are now more closely defined, they vary considerably. There is a diversity of strengths and weaknesses among the major actors, which creates both complementarities and controversies. Yet, most actors have a vested interest in preserving a unified Internet on which convergence can be build.

- More specifically, there are 10 areas of development that we will need to watch closely in 2018: the EU's General Data Protection Regulation and the role of data at the centre of digital politics, the digital politics of cybersecurity, digital trade and the Internet economy, courts as makers of digital rules, artificial intelligence, cryptocurrencies, content policy between countering extremism and fake news, net neutrality and the global impact of US regulations, encryption, and developments related to the Internet Corporation for Assigned Names and Numbers (ICANN).

Filling policy gaps

The gaps in global rules are increasingly filled by bilateral and regional arrangements, in particular on cybersecurity and e-commerce. Plurilateral digital trade arrangements are being considered as an alternative to the shortcoming of the WTO e-commerce negotiations.

In 2018, however, national legislation and courts will have a major impact on the global Internet. For example, we will continue dealing with the ramifications of the US net neutrality ruling and Chinese cybersecurity law. The main regulation with global impact will be the entry into force of the EU's General Data Protection Regulation (GDPR) on 25 May, which will determine how data is governed in the EU as well as and beyond its shores.

The trend of the growing importance of court rulings on global digital policy will accelerate in 2018. In addition to the traditionally active Court of Justice of the European Union (CJEU), courts in Canada, Brazil, and other countries have also introduced rules which are *de facto* new rules of Internet governance.

While changes are certain, their impact is not. Will they lead towards the Internet being a societal enabler or a space for new monopolies? Will the Internet remain unified with the possibility of accessing any website anywhere or will it divide into national digital realms?

Using divergences to reach convergences

There are a few elements on which to build constructive solutions and some optimism.

First, interests in digital policy are now more clearly defined than a few years ago, when digital ideologies focused only on blue-sky thinking and an 'unstoppable march into a bright digital future'. Today, we know that digital development is not only about bright futures, but also about the fulfillment of the interests and goals of major players, here and now. The good news is that although there are varied interests, most actors have a common interest in preserving a unified Internet.

Governments need to deliver prosperity, stability, and security as part of their social contracts with citizens. A fragmented Internet could slow economic growth and trigger domestic protests.

Industry's main purpose is to make a profit, whether it is by selling services online or by monetising data. Fragmentation of the Internet would oblige them to redirect their resources to crossing new digital borders. Every new digital border will mean less income for the Internet industry.

For many citizens worldwide, the Internet is an indiespensable part of their lives. It is part of daily routines which range from keeping in touch with family, to buying products and services, and voicing advocacy positions and concerns. In extremes, dependency on the Internet turns into addiction. Any major disruption of the Internet would trigger protests from users and social instability.

Three main digital actors also complement each other. Companies have power in the digital realm, but they can easily lose it. Governments do not have as much power, but they may gain it through regulations. Governments and citizens have legitimacy, which companies increasingly lack. Fake news, tax avoidance, and data leaks have tarnished the image of the Internet industry. This diversity of strengths and weaknesses among the major actors creates both complementarities and controversies.

A clear delineation of the interests of all actors, a healthy interdependence, and complementarity between those actors is a good basis for negotiations, compromise, and ideally, consensus, on how the Internet should further develop as a technological enabler of a stable and prosperous society.

Second, the diversity of the Internet is reflected in the diversity of interests and, ultimately, negotiating positions in digital geo-politics. While the USA and Russia disagreed on the future of cybersecurity regulation within the UN Group of Governmental Experts (UN GGE), they did agree about the need for digital commerce regulation in the WTO. The two countries supported the process that may lead towards the WTO plurilateral negotiations on digital commerce. This variable geometry in the positions of the main actors in digital policy could create more space for potential trade-offs and compromise.

10 predictions for 2018

The following forecast of the 10 main digital policy developments is set against this broad backdrop that makes progress and retreat equally possible. It draws on continuous monitoring of digital policy carried out through the *Geneva Internet Platform's (GIP) Digital Watch* observatory and further discussed during the GIP's monthly briefings.[1]

The 10 areas of development that we will need to watch closely in 2018 are: the General Data Protection Regulation and the role of data at the centre of digital politics, the digital politics of cybersecurity, digital trade and the Internet economy, courts as makers of digital rules, artificial intelligence, cryptocurrencies, content policy between countering extremism and fake news, net neutrality and the global impact of US regulations, encryption, and developments related to Internet Corporation for Assigned Names and Numbers.

1. GDPR: Data in the centre of digital politics

Data has always been a salient issue in digital policy, yet its centrality became clearer in 2017, leading *The Economist* to describe data as the 'oil of the new economy'.[2] Like oil, data generates economic growth as well as conflicts, in this case over data access and control. During the 2017 Internet Governance Forum, data was one of the most frequently used words in many sessions, discussing the technological, economic, legal, and human rights aspects of data governance.[3]

When it comes to personal data, the EU's GDPR, which will enter into force on 25 May, will have a major impact this year. A main development in global digital politics, it will have far-reaching consequences on the digital economy, cybersecurity, and human rights online.

The GDPR will introduce very strict regulations on the way the data of European citizens is collected, used, and shared, with fines for breaches of up to €20 million or 4% of a company's global annual revenue.

The GDPR is likely to have a global impact in two main ways. First, the EU is extending its jurisdiction globally by requesting that the data of European citizens be managed according to European regulation, wherever data processing takes place.

Second, other countries may follow suit. With a high Internet penetration of 500 million citizens with strong purchasing power, the EU is the most lucrative Internet market in the world. The EU has the digital 'hard power' to negotiate with Internet companies on an equal footing. Typically, other countries and regions carefully follow the governance battles between the EU and the Internet giants – and their outcomes – and act accordingly. For example, many countries introduced the right to be forgotten after the CJEU judgement from May 2014.

How will the GDPR affect Internet companies?

In addition to creating a shift in favour of privacy in the corporate culture, the GDPR will affect both the current Internet business model based on processing data for advertising, as well as future models based on using data for the development of artificial intelligence (AI).

In the current Internet business model (*Figure 1*) user data is collected, processed, and monetised via advertising. The GDPR requires Internet companies to get consent of users whenever their data is used beyond legitimate business purposes for the performance of the contract (e.g. service customisation). If users decline the monetisation of their data, they cannot be declined the use of Internet services such as Google and Facebook.

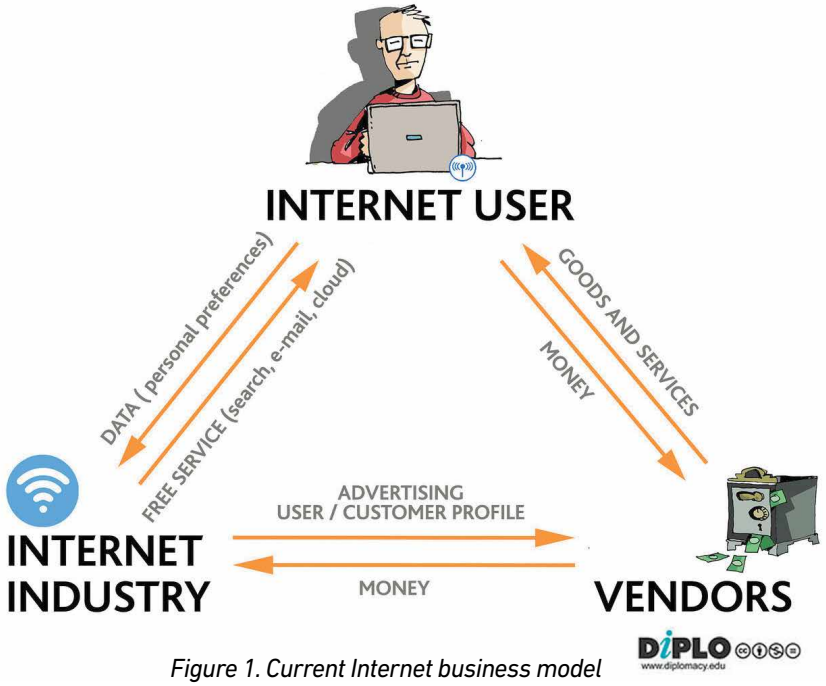

Figure 1. Current Internet business model

Here, the GDPR will challenge the existing tacit deal between users and Internet companies, by which users provide data without any strings attached in exchange for 'free service'. If this tacit deal is challenged, Internet companies may look for some other business models such as charging subscription fees for services. In any future development, the GDPR will significantly challenge the current business model which is based on monetising our data in exchange for providing free services.

In the emerging business model (*Figure 2*), (big) data is collected by Internet of Things (IoT) devices and used for AI development. According to the GDPR, companies can only collect data that are strictly necessary for the performance of contracts. Otherwise, if companies want to use data for data-mining, each company will need the separate consent of each individual or organisation that provides data.

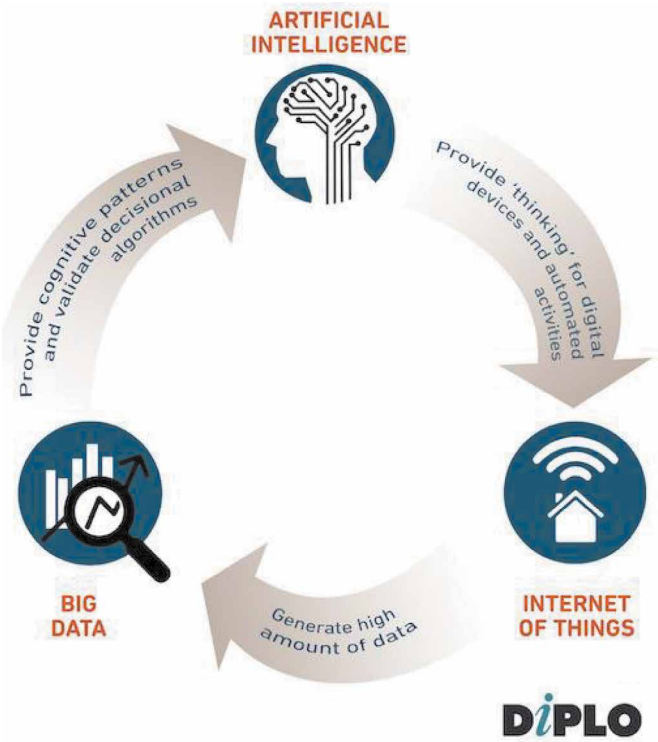

Figure 2. The emerging business model: The interplay between AI, the IoT, and big data

Thus, building a big data collection which is essential for identifying patterns and AI development will become more difficult. One can expect that future court cases will be centred on determining what circumstances are 'necessary for the performance of the contract'.

How to deal with current and emerging business models will be the core question for Mark Zuckerberg while he takes on his 2018 challenge to 'fix Facebook'.[4] The GDPR is the first glimpse of new business challenges for all companies that operate by monetising users' data. If Zuckerberg does not come up with some more creative solution, Facebook may start charging subscription fees, for example. If Facebook decided to charge 10 USD per year to each of its 2.1 billion users, it would generate USD 21 billion – which is twice Facebook's 2016 income of 10.2 billion USD.

Mainstreaming data in traditional policy fields

In 2018, we can expect that data will come more into the focus of specialised agencies and organisations dealing with health, humanitarian, and development issues, among others. The World Health Organization (WHO) will need to address the specificities of data protection and the sharing of health data.

The humanitarian sector (such as the International Committee of the Red Cross and the UN Refugees Agency) will have to continue developing guidelines on balance between data protection and the public interest: data can save lives, but poor data protection could also lead to discrimination and deterioration in personal security.

Development agencies will deal with the sharing of data for the implementation and monitoring of the sustainable development goals (SDGs). While the increasing volume of data provides new opportunities for measuring the 2030 SDG indicators, it also adds complexity to the collection and comparability of such data.

The International Labour Organization (ILO) will have to look into issues related to the rights of employees and the way their data is used by employers, especially in a future of work characterised by increasingly blurred lines between professional and private lives.

Need for interdisciplinary data policy

In 2018, the need for an interdisciplinary approach to data policy will become more obvious (*Figure 3*). For example, trade negotiators may be required to negotiate the free flow of data. In practice, trade arrangements could be restrained by other regulations, such as those on the protection of privacy, standardisation, or security.

The free flow of data could be restricted by regulation on fake news, which is currently being considered in several countries. Technical data standards could impact the security, economic, or human rights aspects of data governance.

So far, there is no space where data can be addressed in multidisciplinary ways on regional or global levels. Even at national level, data policy remains a challenging task, involving trade, security, telecommunication, cultural, and other ministries.

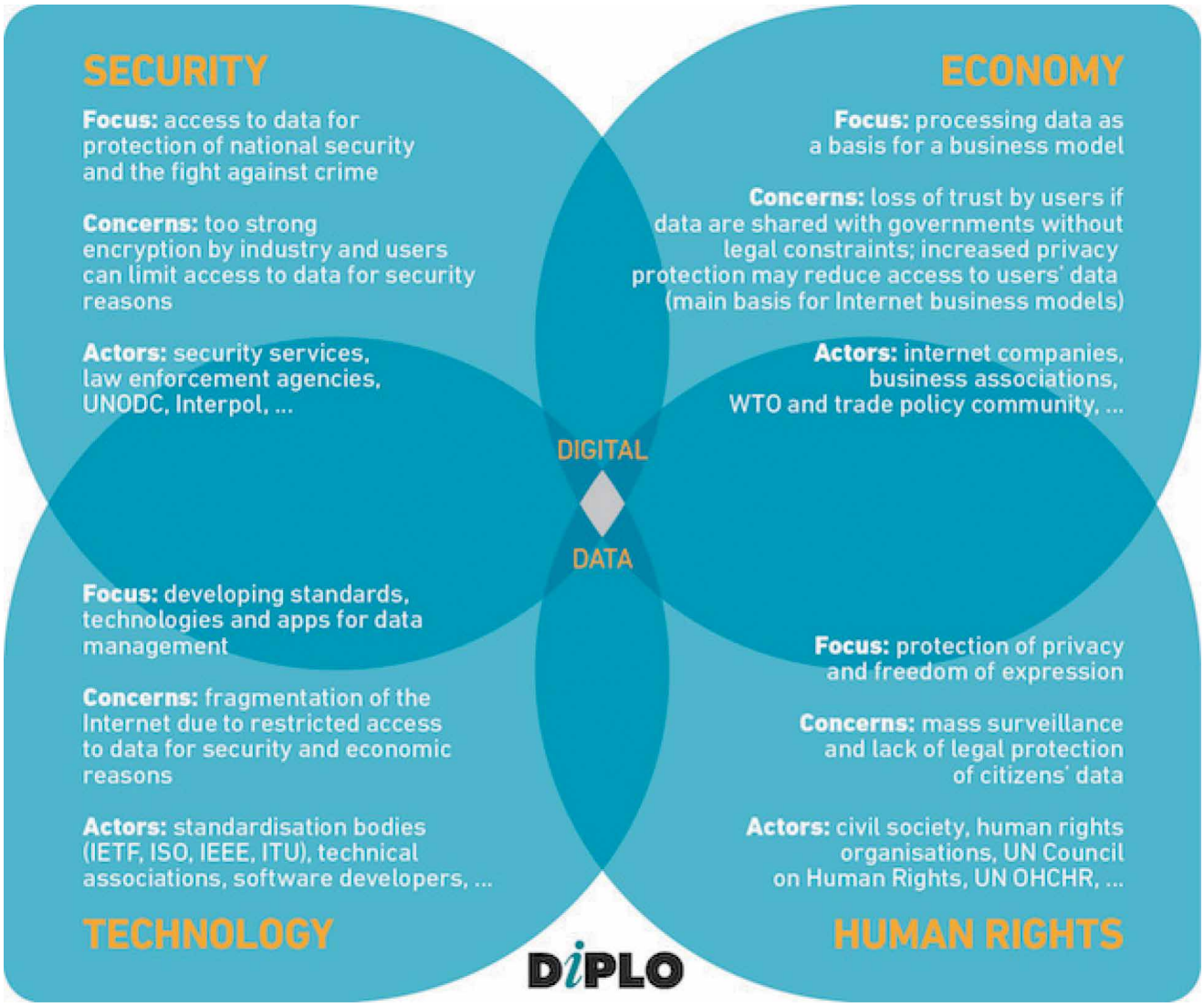

Figure 3. Multidisciplinary data governance

2. Cybersecurity geopolitics: The search for new governance mechanisms

By the end of 2017, the Internet was less secure than it was the previous year. Critical vulnerabilities are more frequently exploited now, increasing the risks for society. The most severe exploitation of a vulnerability was the WannaCry ransomware attack, which infected hundreds of thousands of computers around the world.[5]

Additional risks emerged with vulnerabilities like Spectre and Meltdown that affected the core hardware/software architecture of millions of computers and digital devices worldwide. Infrastructure policy solutions lagged behind new cybersecurity risks. The UN GGE failed.

Regional initiatives will try to make up for the lack of global initiatives. Increasing cybersecurity costs and business risks will make Internet companies step up their search for cybersecurity solutions. Microsoft's proposal for a Digital Geneva Convention will continue to be debated triggering more discussion on open and controversial issues. While the search for cybersecurity solutions continues, a lot will be done in capacity development and application of existing norms and policy mechanisms in the field of cybersecurity.

A growth in cybersecurity risks

In 2018, cybersecurity risks will increase. The growth in the number of Internet users is unlikely to be followed by increased cybersecurity awareness. Critical systems, especially in developing countries, continue to use vulnerable platforms, including old applications with no security updates available.

The Internet economy will further add to cybersecurity risks. Strong competition accelerates a 'release the product now, patch later' approach, with the proliferation of critical vulnerabilities as a result. In addition, the fast-growing IoT market will create a new range of cybersecurity risks, as products are often produced by non-IT companies and without 'security by design'.

Without an efficient system and defined responsibilities to report and handle critical vulnerabilities of new software and IoT, vulnerabilities may be secretly stockpiled by states or other actors, and leaks can deliver information to the hands of criminals, terrorists, and perpetrators of cyber attacks.

Cybersecurity risks will be increased as more countries invest in offensive cyber-capabilities. According to Diplo's recent study on trends in cyber-armament, there are 20 countries for which it can be claimed with certainty that they have offensive capabilities, while there are indications that other countries are in possession of such capabilities (*Figure 4*).[6] Cyber armament and big budgets will drive the security industry to produce offensive cyber tools. Due to increased public pressure, some countries might move to more transparency on their cyber capabilities and policies related to vulnerabilities, storing, and using cyber-weapons and offensive capabilities.

Policy solutions for cybersecurity

After the failure of the UN GGE to reach consensus over a report in 2017, the search for global cybersecurity mechanisms will intensify in 2018. Based on the experience of five UN GGE meetings (since 2004) and other cybersecurity processes, the future solution should be broad enough to ensure inclusiveness and focused enough to ensure effective deliberations. An inclusive process will enhance the legitimacy of an agreed outcome. In addition, it will contribute to the social incorporation of agreed norms by policy communities and the general public. Without societal buy-in, it will be difficult to implement new cybersecurity norms and policies.

At the same time, the inclusion of more actors around the table could slow down negotiations. Wider participation might not be ideal for finding applicable solutions, which are usually found in smaller expert groups. These potentially contradictory requirements for inclusion and efficiency should be kept in mind while searching for balanced mechanisms for cybersecurity policy. The current menu features a number of proposals, options, and ideas:

Continuation of the UN GGE process

This option would involve conveying a 6th UN GGE in September 2018, although generally speaking, there is no appetite for more of the same. Proposals for the next UN GGE include:

Mandate: Russia suggested that the UN GGE drafts a Code of Conduct; other possibilities focus more on operationalising the 2015 UN GGE report.

Modus operandi: increase the number of members, develop informal consultations prior to the UN GGE meetings, and find ways to involve technical experts and civil society.

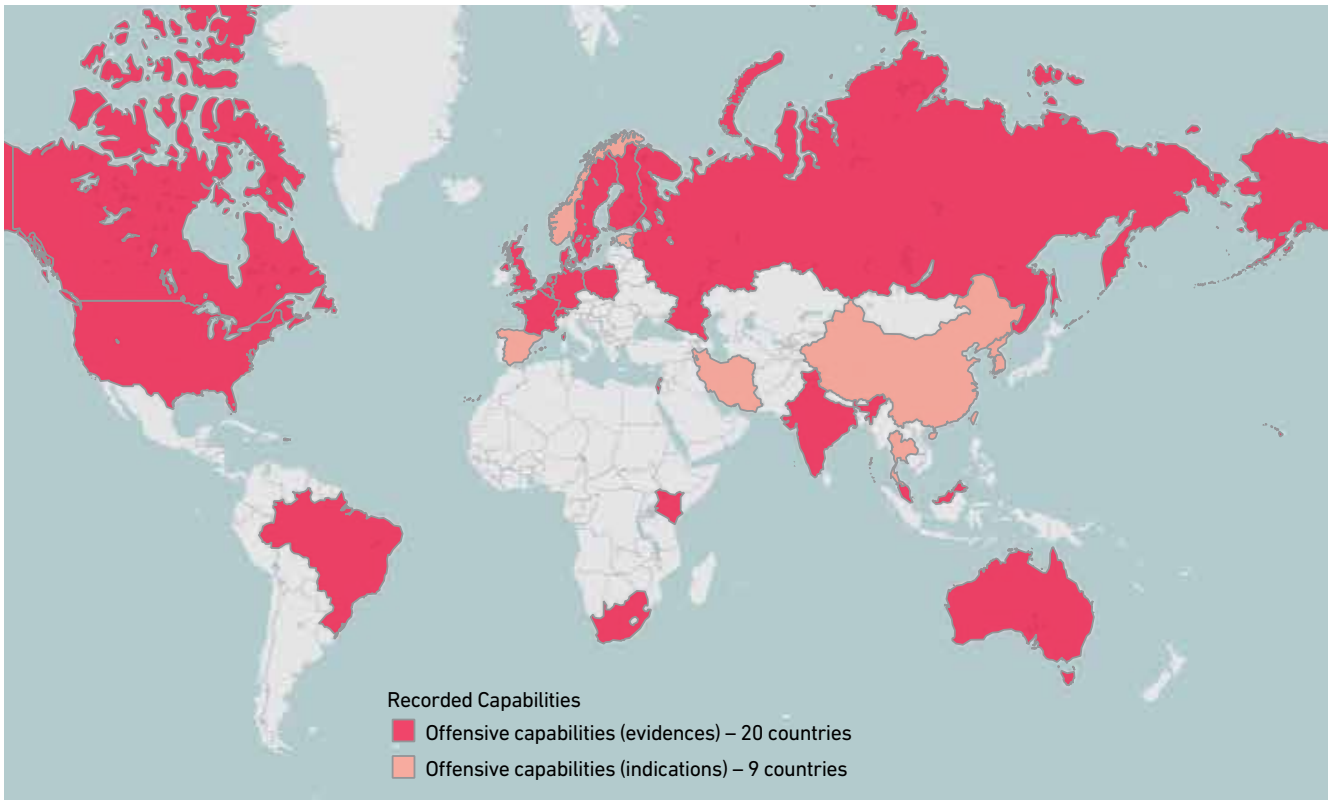

Figure 4. Map of offensive cyber capabilities[7]

UN Open-ended Working Group on ICT security

The Group of 77 proposed an Open-ended Working Group on ICT Security in the framework of the UN General Assembly (UNGA).

> Mandate: Harvest a wide range of proposals, including points of consensus and disagreement, to develop actionable recommendations that may include a proposal for drafting a cybersecurity treaty.
>
> *Modus operandi*: Use UNGA rules for open-ended groups to ensure a high level of inclusion, transparency, and legitimacy with the participation of all member states, non-governmental actors, and the private sector.

UN Conference on Disarmament

There is a formal possibility to include cybersecurity in the activities of the UN Conference on Disarmament (CD). China raised the question of cybersecurity in a CD. However, due to the current stalemate in the work of the CD, this is not a viable option for the advancement of cybersecurity discussions. Even if it were possible, the CD would have serious limitations with regard to inclusivity and transparency.

International Telecommunication Regulations

Following a recent Chinese proposal for a meeting of the Expert Group on International Telecommunication Regulation (ITRs), ITRs are likely to be considered as one of the possibilities to deal with global cybersecurity. As a recent analysis by telecom expert Anthony Rutkowski indicates, the Chinese proposal tries to address the emerging cybersecurity issues – particularly the increasing virtualisation of networks (such as with cloud solutions) across jurisdictions by transnational companies, and their attempts to build vast collections of personal data of citizens.[8] Rutkowski argues that China is trying to fill the gap (whether perceived or real) created by the USA's objection to the establishment of an international instrument on cybersecurity.

This comes as a result of the expanding global presence of the Chinese digital industry – for instance, leading Chinese companies such as Huawei, ZTI, and China Telecom are also part of global industry efforts to standardise virtualisation technologies.[9] Cybersecurity may figure prominently at the next ITU Plenipotentiary meeting in Dubai in November. Given the lack of consensus, differences could trigger different blocks as happened, incidentally, in Dubai during the ITR negotiations at WCIT 2012.[10]

A Committee on the Peaceful Uses of ICT (COPUICT)

Cyber governance can benefit from experience in the field of outer space. In 1959, the UNGA established a Committee on Peaceful Uses of Outer Space (COPUS) to 'govern the exploration and use of space for the benefit all humanity: for peace, security and development'.[11] A COPUICT framework could anchor digital discussion in the UN functional trinity: peace, security, and development. Analogous to outer space, COPUCIT could focus on scientific, technical and legal issues. It could also provide policy research and analysis of legal problems from cybersecurity and other digital fields. COPUICT could play a prominent role in coordinating the capacity development efforts of numerous actors worldwide. COPUCIT could carry out its activities through an annual meeting and the establishment of ongoing sub-committees. Its activities should be closely coordinated with the Global Forum on Cyber Expertise (GFCE), Internet Governance Forum, Commission on Science and Technology, ITU and other organisations involved in cybersecurity and wider digital policy fields.

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. The question remains how to achieve a better synchronisation between global and regional efforts, as discussed in a research paper by Diplo and the GIP.[12]

In addition to already advanced cybersecurity cooperation efforts (e.g. OSCE, ASEAN Regional Forum, the Organisation of American States, and the Shanghai Cooperation Organisation), there is a need to strengthen the cybersecurity processes of other regional actors, and particularly the African Union, since its Convention on Cyber Security and Personal Data Protection, adopted in 2014, has so far been signed by only nine countries and ratified by one.

Private sector initiatives

The business sector is most vulnerable to cybersecurity risks. Cybersecurity budgets are growing quickly. Vulnerabilities threaten the business model of the Internet industry. Thus, one can expect an acceleration in business cybersecurity initiatives in 2018. Technical attribution of cyber-attacks will be a high priority, with the main challenge being how to ensure that technical attribution triggers legal and policy actions. Given its consequences, any discussion on attribution will be highly politicised. This question of addressing the attribution of cyber-attacks is one of the main pillars of Microsoft's proposal for a Digital Geneva Convention.[13]

In 2018, Microsoft is likely to focus on gathering the support of the Internet industry if it wants to make this proposal appealing to governments worldwide. Google will also work on new norms and procedures for providing digital evidence to foreign governments in a more efficient way than by using the traditional Mutual Legal Assistance Treaties (MLATs).[14]

Other policy initiatives

The Global Commission on the Stability of Cyberspace will continue working on new norms and proposals after recently issuing a Call to protect the public core of the Internet, and garnering the support of some states.[15] If it consolidates its internal cybersecurity structures, the USA may develop further its idea to gather a 'coalition of the like-minded' and look for ways to conduct attribution jointly, and enforce the implementation of existing norms.[16]

The members of the Shanghai Cooperation Organisation will continue working on the Code of Conduct for Cybersecurity. At the same time, Russia will continue its efforts to discuss its draft Universal Convention on Countering Cybercrime, while more countries worldwide are likely to access the existing Budapest Convention of the Council of Europe (currently ratified by 47 member states, plus 24 non-member countries).[17]

At the IGF 2017, Switzerland announced a policy and research project which would focus on responsibilities in cyber matters of governments, business, and users.

Capacity development

Capacity development remains the least controversial topic in cybersecurity negotiations. Thus, while policy solutions are negotiated, there will be continued efforts to build capacities and competencies such as those by the Council of Europe (for law enforcement), CERT (Computer Emergency Response Team) communities, the GFCE, the ITU, the IGF, Internet Society and the Geneva Internet Platform, among many others.

Enhanced communication and coordination among these initiatives, particularly within the IGF and the GFCE, is expected.

3. Digital trade and the Internet economy

E-commerce ranked high on the thematic priorities of the WTO throughout the year, confirming our predictions for 2017.[18] In spite of these priorities, the WTO Ministerial Conference (Buenos Aires, 10–13 December) failed to produce a final declaration or to agree on an update to the nearly 20-year-old Work Program on Electronic Commerce, approved in 1998.[19] The moratorium on customs duties on electronic transmissions was renewed at the last minute of the WTO Ministerial Conference.

There are persistent differences of viewpoints between, on one side, mainly developing countries, which argue that negotiations on e-commerce should not be initiated before the development-related goals of the Doha Round are further advanced, and on the other side, a rather diverse group of more than 70 countries, arguing for adoption of more robust rules on e-commerce at the WTO. These countries, including the USA, Russia, and the EU, agreed in Buenos Aires to 'initiate exploratory work toward future WTO negotiations on trade-related aspects of e-commerce', which could indicate the start of plurilateral negotiations on digital trade.[20] In 2018, the main issue will be how this group will set parameters for negotiations between core commercial issues and wider digital policy issues (*Figure 5*).

Some voices in civil society are concerned that, through digital trade, this plurilateral group may try to regulate a wider scope of digital policy issues, such as cybersecurity, data governance, and human rights.

In parallel to the WTO dynamics, several regional and mega-regional trade agreements are being negotiated at varying speeds. Most of them include chapters dedicated to e-commerce. The potential stalemate of multilateral discussions could serve as an incentive for trade-related digital issues to further percolate into these regional treaties, which already include provisions on the topics of disclosure of source code of digital products, encryption, data flows, and data localisation.

The importance of data to digital trade is becoming increasingly clear. The 2017 Information Economy Report, published by UNCTAD, calls attention to the importance of big data, the IoT, and AI to the future development of the digital economy.[21] It also alerts readers about the potentially negative effects that emerging technologies could have on the distribution of revenues between the developed and developing worlds and on the disruption of the job market.

In addition to impact from data governance issues, the taxation of the Internet economy is another issue which will remain high on the digital agenda, in particular in the EU. In 2018, member states will try to find a solution among three possibilities outlined during the Estonian presidency of the EU: an equalisation tax (proposed by 'the big four': France, Germany, Italy, Spain), virtual permanent establishment of companies (proposed by Estonia), and retaining the status quo (proposed by Ireland, Luxembourg, and Malta). Outside of the EU, Indonesia and Russia, among other countries, prefer to use the presence of Internet companies in a national jurisdiction as the basis for operations and taxation.

Following the request for public input on the Inception Report, the ILO High-Level Global Commission on the Future of Work will further explore an impact of digitalisation on jobs.[22] In particular, we can expect discussions on the status of workers in the context of the sharing economy,

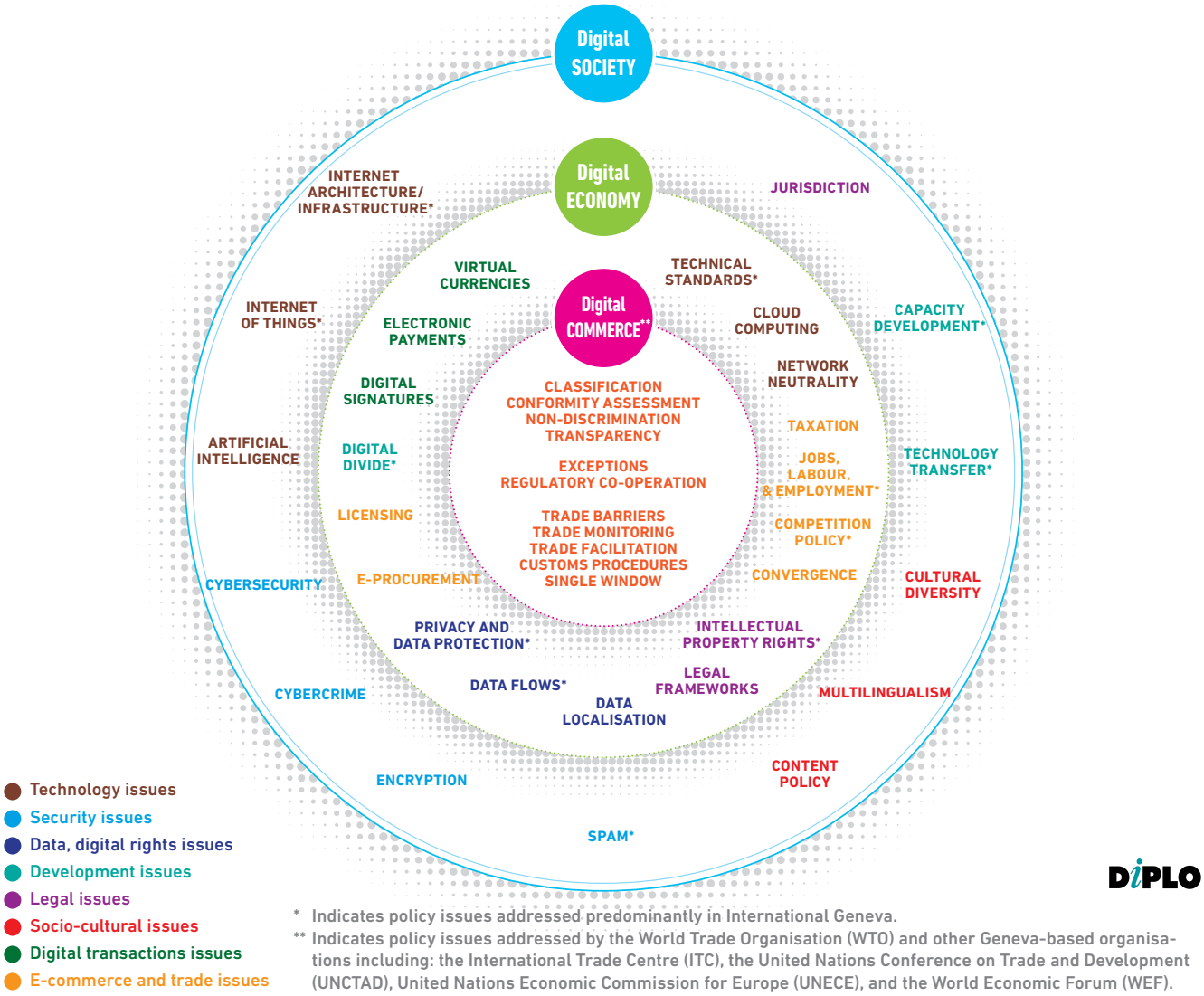

Figure 5. Three different circles showing the relevance of digital policy issues for digital commerce

precarious jobs, social security systems, and social justice arrangements in the world of work more generally.

The Internet, automation, and AI are among the key shapers of the future of jobs. The main impact of technology on the manufacturing sector is already being seen, with more than 80% of the work in the manufacturing sector being performed by robots in developed countries. In the developing world, the nature of work is also changing, leading to further discrepancies in job quality and job quantity. Technology-driven transformations also include digital labour, regularly enabled by a platform (crowdsourced or sharing economy model). What is at stake in 2018 is rendering the online tasks performed by millions worldwide visible and protecting them in accordance with minimum welfare standards.

List of actors initiating plurilateral negotiations on digital trade at the WTO

Albania, Argentina, Australia, Bahrain, Brazil, Brunei, Cambodia, Canada, Chile, Colombia, Costa Rica, European Union, Guatemala, Hong Kong, China, Iceland, Israel, Japan, Kazakhstan, (South) Korea, Kuwait, Laos, Liechtenstein, Macedonia, Malaysia, Mexico, Moldova, Montenegro, Myanmar, New Zealand, Nigeria, Norway, Panama, Paraguay, Peru, Qatar, Russia, Singapore, Switzerland, Taiwan, Turkey, Ukraine, United States, Uruguay

4. Courts: Active maker of digital rules

Numerous court rulings on digital issues confirmed our predictions for 2016 and 2017, namely 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, as was the case with the right to be forgotten.[23]

In 2018, the CJEU is expected to keep its prominent role after ruling in previous years on the right to be forgotten and privacy protection. On 20 December 2017, the CJEU ruled that Uber is a transportation company, rather than an information society one, as the company had argued. As a transportation company, Uber will need to follow national transport regulations, and its business model will be deeply affected. Moreover, as has happened in the past, it is very likely that other countries outside Europe will regulate Uber's activities in a similar way. The study *Mapping Uber: a database of court cases and rulings* illustrates that Uber is involved in legal action over several issues in more than 25 countries (*Figure 7*).[24]

Other courts will start addressing digital cases, continuing the trend from 2017 when courts in Austria requested that Facebook remove legally prohibited content not only in Austria but also worldwide.[26] Courts in France and Canada requested that Google remove search results worldwide for content legally prohibited within their own jurisdictions.[27] This prompted Google to ask if it is fair and appropriate for national authorities to decide what should be accessed in other countries beyond their jurisdiction.[28] An Australian court ordered Twitter to prevent a particular user from opening a Twitter account anywhere in the world.[29]

The following digital issues are likely to be covered by courts in 2018: cybercrime, content removal, the role of intermediaries, freedom of expression, protection of personal data, mandatory data retention requirements, and mass surveillance, to name a few.

Figure 6. Digital Justicia

During the next few years, we can predict that governments will bring the first Internet-related case to the International Court of Justice in The Hague. The following issues could be in the focus of such court case: cybersecurity incidents, territorial integrity in cyberspace, protection of the Internet cables, and access to data.

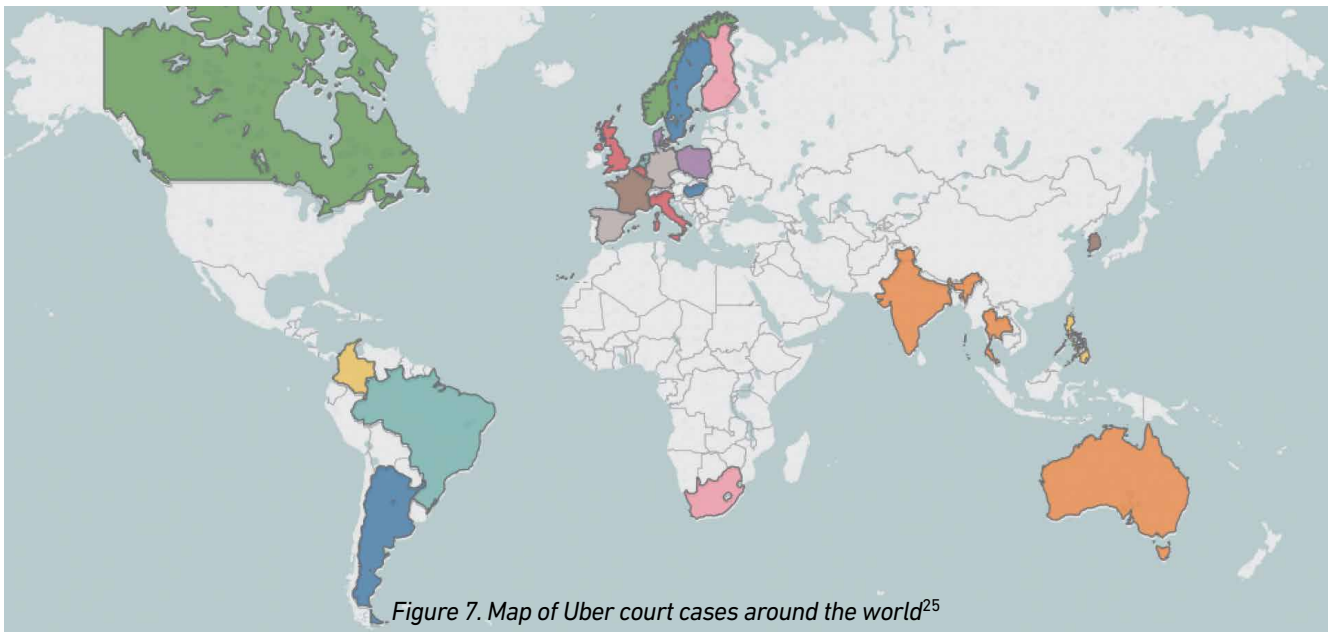

Figure 7. Map of Uber court cases around the world[25]

5. Artificial intelligence: Between philosophical considerations and practical applications

AI triggered a very wide and controversial discussion in 2017, which was summarised by Stephen Hawking saying that AI may 'be the best or worst thing to ever happen to humanity'.[30]

On the best side, AI has the potential to make our life easier. It can provide better diagnostics (AI in radiology), smarter decisions (data mining), and easier daily life (personal assistant). It is even argued that, combined with other technologies (such as IoT), it could help identify sustainable solutions to some of the world's most pressing problems, such as poverty, hunger, and climate change.

On the worst side, AI could make wars and human suffering even worse through the use of lethal autonomous weapons. It could also challenge the central role of human will and reason in society. One of the most alarming views came from Tesla CEO Elon Musk who told US governors that AI 'is a fundamental existential risk for human civilisation', and that there should be proactive government intervention.[31]

In 2018, this debate will accelerate. Most likely, there will be more philosophers addressing ethical dilemmas. The main challenge will be to have as informed and balanced discussions as possible, by bringing into the debate technical experts who can distinguish between hype and reality in AI, philosophers who can revisit some cornerstones of ethics and epistemology in the context of AI development,

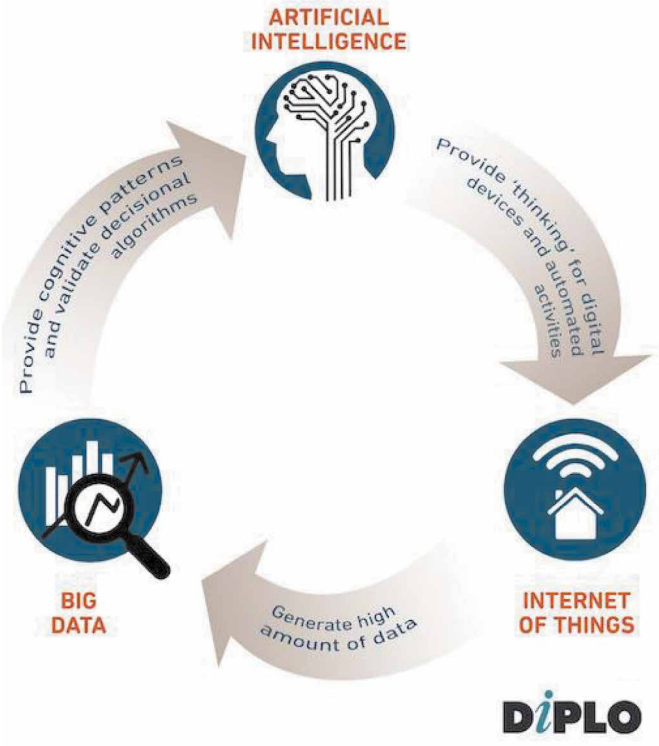

Figure 8. Interplay between AI, the IoT, and big data[32]

technology companies that are the main engine behind AI growth, politicians who should galvanise public support, civil society who will defend human rights and equity, and the general public which will be inevitably affected by AI.

While the future is there to be discovered, in 2018, one can envisage the many policy discussions on AI. One such discussion will be about addressing the powerful interplay between AI, big data and the IoT as illustrated in *Figure 8*.

First, AI provides 'thinking' for IoT devices and gadgets. It is what transforms cars, for example, from dumb vehicles operated by a driver to intelligent driverless vehicles. Second, smart devices and the IoT generate a lot of data, sometimes labelled as big data, which is used for data analysis. Insight from data generated by users is the cornerstone of the business model of the major Internet companies (Google, Facebook, Twitter). Third, the circle is closed by the verification of initial AI algorithms based on user-generated data gathered through smart devices. In addition, data analysis identifies cognitive patterns that could be integrated into new AI algorithms.

As the interplay between AI, the IoT, and big data becomes increasingly powerful, concerns are also growing about its implications for the economy, social welfare, privacy, safety and security, and ethics, among others. Initiatives are emerging, across all stakeholder groups, with a focus on identifying ways to address such concerns, as the following examples illustrate.In April 2017, the UK's Royal Society called for careful stewardship of machine learning (the technology that allows AI to learn from data) 'to ensure that the dividends from [this technology] benefit all in the [...] society'.[33]

The power of this emerging business model led major Internet companies (IBM, Facebook, Google, Microsoft, Amazon, and DeepMind) to launch the Partnership on Artificial Intelligence initiative, aimed at addressing both AI opportunities and risks.[34] On the opportunities side, there are more and more examples of effective use of AI such as Microsoft's project on AI for Earth and a Research AI lab.[35] Facebook is using AI to tackle online content related to terrorism.[36]

On the risks side, the private sector is addressing questions of privacy, security, and ethical challenges of AI. For example, Google has been undertaking research on issues such as addressing privacy concerns in AI solutions.[37]

Governments also have become more aware of the significant potential that AI and the IoT have for development, and are looking into ways to support the evolution of these fields. China, for example, who has long supported research in

the field of AI, has released a national AI development plan, intended to make the country the world leader in the field by 2030.[38] In Russia, President Vladimir Putin spoke about the country's efforts to achieve excellence in AI, and said that 'artificial intelligence is the future, not only for Russia, but for all humankind'.[39] It is likely that more countries will start placing AI at the core of their development strategies.

For the legislators, the focus will be on determining whether current regulations and legislation – in areas such as labour market and social security, safety and (cyber) security – are sufficient (at least for the time being) to tackle the implications of AI, or whether new policy frameworks are needed, to address, for example, issues of liability and accountability in the context of automated systems.

The development of lethal autonomous weapons will also be tackled by the Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), which is expected to continue the discussions started in 2017 on issues related to technological, military, legal, and ethical considerations.[40] During the 2017 meeting, there were calls for a moratorium on the deployment of LAWS; support for such a moratorium is likely to gain traction, following the call for a ban on LAWS made by more than 100 AI pioneers in 2017.[41] The Group will meet again in April and August 2018.

Judging by developments in 2017, it is likely that debates will intensify in 2018 on issues related to taxation (Is the taxation of robots a viable solution for alleviating some of the social implications of AI and automation developments?) and the legal status of automated systems (If we grant citizenship, residency, or another legal status to automated systems – as it was the case with robot Sophia and chatbot Mirai in 2017 – what do we really gain from this?).

6. Bitcoin and cryptocurrencies: Between boom and bust

In 2017, one of the main surprises was the fast rise of the cryptocurrency market. The first and most prominent cryptocurrency, Bitcoin, rose from USD 970 per bitcoin on 1 January to USD 13,700 on 31 December 2017. More cryptocurrencies emerged, such as BitcoinCash, IOTA, and Cardano, alongside the other main players in the field: Ether, Ripple, and Litecoin.

At the end of 2017, the Bitcoin market cap was raised to USD 230 billion, and the whole cryptocurrency market cap increased to USD 700 billion.The main question for 2018 is: Will the cryptocurrency boom continue or will the cryptocurrency bubble burst? Those who argue that the boom will continue and that cryptocurrencies are here to stay often point to the trust created through a distributed network (no one person can easily manipulate it), as well as the high functional compatibility of cryptocurrencies with the Internet economy (global nature, easy access). The other camp argues that cryptocurrencies are not currencies in the traditional sense, because their value changes

Figure 9. Growth of Bitcoin in 2017[42]

Position and Regulation on Digital, Crypto and Virtual currencies

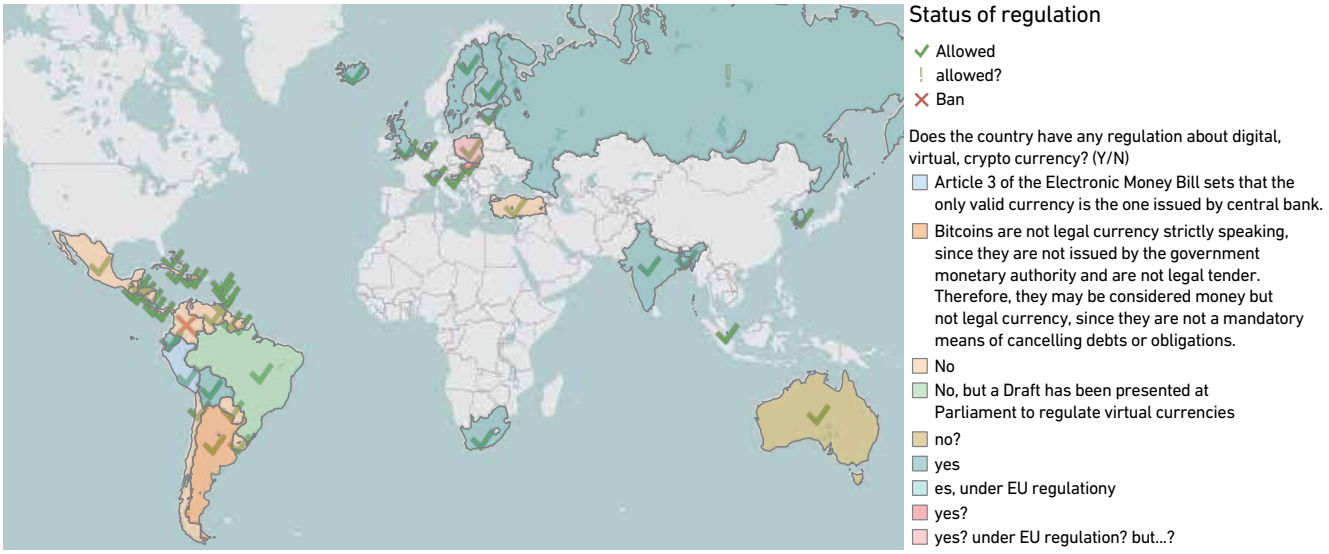

Figure 10. Position and regulation of digital, crypto and virtual currencies

dramatically; they are just another bubble triggered by a mix of digital fashion and the availability of uncommitted capital, in particular, owned by high-tech venture capitalists and high-tech companies. Also, there is criticism of so many decentralised solutions (blockchain boom) which now, many years after their start, have not produced any major and practical use case of global implementation of blockchain technologies.

Some argue that money laundering also contributed to the cryptocurrency bubble. While it is difficult to predict boom or bust scenarios, governments will start addressing some governance issues that could affect the financial market and the wider economy.

First, states will try to regulate Bitcoin and other cryptocurrencies in exercise of their monetary and financial authority. The first target of regulation will be the so-called Initial Coin Offering (ICO), a system for raising money from the public through a process of issuing virtual tokens that can be traded on online cryptocurrency exchanges. ICOs are similar to an Initial Public Offering (IPO). Unlike IPOs, however, ICOs are unregulated, and do not undergo the same auditing and regulatory scrutiny. South Korea and China have temporarily banned ICOs. Australia, Canada, and the USA have imposed regulations. India, the EU, Singapore, and others have issued warnings for investors and firms involved in ICOs, and many other countries are preparing proposals for regulations. The main focus of regulators will be on fraud protection for investors and full data compliance for companies.

Secondly, anti-money-laundering authorities will pay more attention to cryptocurrencies in 2018. Tax collecting agencies are developing sophisticated methods of blockchain monitoring and collecting data on user profits. Various sanctions regimes will also focus on the use of cryptocurrencies to avoid economic sanctions as allegedly happened with sanctions against Venezuela and Russia.

Thirdly, there will be more discussions on establishing national cryptocurrencies. Vitalik Buterin, the founder of Etherium, a leading cryptocurrency, argues that 'So far, there is nothing close to a central bank issued digital currency.' Governments are not likely to pass their monetary responsibilities over to a transparent and unchangeable system beyond their control.

7. Content policy: Fake news and violent extremism online

Fake news was the word of the year in 2017 according to Collins Dictionary.[43] In 2018, it is likely to remain central in public debates, in relation to both semantics (as many argue that the term 'fake news' lacks clarity/accuracy, and other terms, like misinformation or information disorder, would be better suited to describe the phenomenon) and policy approaches. Addressing fake news, together with violent extremism content, is a matter of content policy, and could have significant implications for the role of Internet companies as intermediaries, as well as for freedom of expression.

In 2018, governments will increase pressure on Internet platforms to take responsibility for the content they host. G7 members states would like companies to remove violent extremism content within 1–2 hours of it appearing online. It poses a practical challenge for companies to identify such content and the risk that 'legitimate' content may

be deleted. Governments are increasing rhetorics such as UK Security Minister calling Internet companies 'ruthless profiteers'. The current trends are likely to develop further.

First, companies will continue dealing with content issues on a voluntary basis as much as possible, to avoid being forced to do so via regulation. In this direction, several initiatives have already been developed. For example, Facebook, Microsoft, Twitter, and YouTube formed a Global Internet Forum to Counter Terrorism. Internet companies joined forces with French news organisations to combat fake news.[44] Companies are also working on developing automated solutions using AI and algorithms to identify and deal with problematic content. Such 'censorship by industry' may trigger reactions from civil society who feel that it might violate the right to freedom of speech.

Secondly, some governments have started introducing regulations that deal with questionable content. In Germany, Internet companies with more than two million German users must remove 'obviously illegal' content within 24 hours or risk a fine that could rise to €50 million.[45] French President Macron announced new legislation against fake news for 2018, and the EU has announced that it will increase its pressure on Internet platforms. The UK and other countries have warned Internet companies that they will be penalized if they do not find a solution for violent extremist content.

One of the main criticisms of the regulatory approach is that it could endanger freedom of expression. As 'illegal content' and 'fake news' are terms that are not yet clearly defined, Internet platforms might be too eager to remove content in order not to risk a major fine. This practice may infringe on freedom of expression. Voluntary solutions developed by the industry could have a similar effect; for example, it might be difficult to question decisions on the removal of content that are taken by automated systems.

Thirdly, in 2018, we can expect some more in-depth discussions on how society can address the impact of fake news on the robustness of public policy debates. The best medicines for fake news are critical thinking and digital literacy, which, combined, would help citizens to validate information. Ultimately, this should result in creating a more robust public debate space. This approach could provide a solid, long-term solution.

8. Net neutrality: Global impact of new US regulation

The overturn of net neutrality rules in the US dominated tech media coverage at the end of 2017. The US Federal Communications Commission (FCC) decision to rescind network neutrality protections on 14 December triggered fierce debates, including views that this decision may mark the end of the Internet as we know it.

One important argument in the public debate relates to the differentiated treatment of Internet traffic. On the one hand, differentiation may lead towards different Internets. There might well be a 'VIP Internet' with much faster speeds, more powerful applications, and the latest content for those who can pay, and an 'Internet for the masses' with inferior services and zero-rating-like dangers for those who cannot cross this dollar divide.

Others argue that net neutrality is an attempt to redistribute the 'Internet cake' between Internet companies who provide content and get most of the income, and telecommunication companies who provide the pipe through which content flows, but get a much smaller piece of the cake. Without net neutrality, telecommunication companies would be able to charge content companies for delivering their services.

Yet, others are beginning to argue that basic Internet access should be provided as a public service, as are roads, water distribution, electrical power distribution, etc. This would imply a return to strong regulation of at least the last mile (that is, the final leg of the telecommunications networks that delivers services to retail end-users).

The importance of these points lies in how they truly impact the user: Will users have a choice about the services they receive? Will access be distorted without their knowledge and agreement? Will a user change from one service provider, let's say, Netflix, to another, like Hulu, because Netflix is slow, without realising that it is because their Internet service provider (ISP) owns Hulu, and is slowing Netflix down to give Hulu an edge?

In the case of many services, microseconds are important. Traffic management may no longer be used for enhancing efficiency, but for building financial empires. With the increasing monopoly of some content and service providers (often titled over-the-top or OTT), a parallel question also emerges: As it may become easier to change the ISP than the service (say Facebook or Google), can dominant OTT start conditioning ISPs? And how could this impact the outreach and quality of smaller or emerging services, especially local companies, that do not have such power?

In 2018, opposing views will be re-calibrated to take into account the evolution of business models in the fields of Internet traffic carrying and access provision. First, both Internet and telecommunication companies are extending their services vertically. Dominant Internet companies are laying fibre optic cables and providing wireless access (Google's fibre project in the US is one example). Major telecom companies are also entering the content market (e.g. Verizon acquiring Yahoo!). Thus, it is very likely that there will be competition among vertically integrated players

with the main focus on acquiring as much user data as possible. In addition to current practice on collecting data by content providers (Facebook, Twitter, WeChat), data will also be collected by telecom companies while travelling through their cables. This will heavily impact the sides taken by major players in the net neutrality debate in the future.

A second and related point is that the original Internet architecture is fast-changing. Traditionally, Internet packets would reach their destination via traffic routes (backbones and telecom operators) that connect the content provider and the endpoint.

Today more than 50% of Internet traffic is delivered via Content Delivery Networks (CDNs) – consisting of technical facilities placed at major Internet Exchange Points and telecom providers, containing copies of the most frequently accessed content by users of the region – operated by companies such as Akamai or content providers themselves (e.g. Facebook, YouTube, Netflix).[46] It is important to note that, by most existing regulations, net neutrality provisions address the end-user connection to the ISP (last mile), not the traffic flow between ISPs themselves and ISPs and content providers. The Body of European Regulators for Electronic Communications (BEREC) explicitly indicates this focus on 'the last mile' in the EU net neutrality regulation.[47]

Net neutrality does not exist at an international level. But, any decision by the USA, where many traffic carriers have their headquarters, could influence the approach of other countries worldwide.

In 2018, discussion on technical net neutrality may lose relevance if compared to other issues, such as dealing with fast emerging monopolies built around data, the protection of data and privacy, or promoting cybersecurity.[48] These issues will not be mitigated by having technical net neutrality, meaning equal treatment of traffic, but by the legal and policy responsibilities of major actors in the digital society, ranging from governments to companies and citizens.

On top of it all, it is likely that we will see increasing discussions on platform neutrality or data neutrality. As the big Internet companies become ever more dominant and integrate various platforms and services (e.g. Google holds search engines, translation, document sharing, Android OS), they – not the ISPs – will increasingly be the ones that set the rules of the game and possibly introduce various forms of prioritisation of the services and content they distribute. The importance of neutrality of the application level may gradually overshadow the neutrality of the protocol level, and it may be even harder to address through policies than regulating the work of the telecom sector.

9. Encryption: More pressure on backdoor access

Encryption has been extensively used by Internet companies and users. Following the Apple-FBI controversy in 2016, the adoption of end-to-end encryption by Internet companies became more widespread. This push towards stronger encryption was aimed at rendering eavesdropping more difficult.

Government-led surveillance will be under scrutiny when the Special Rapporteur on the right to privacy, Joseph Cannataci, tables his draft legal instrument on surveillance. Plans to publish a draft were announced in his report to the Human Rights Council last year. It is expected that the report will focus on human dignity offline and online, and will carry measures to ensure that surveillance mechanisms offer the adequate safeguards to users' privacy and other rights.

In parallel, the controversy over strong encryption – in which users, governments, and Internet companies are the main players – governments argue that strong encryption reduces the ability for law enforcement authorities and security agencies to conduct their criminal investigations and anti-terrorist activities effectively. The FBI has called encryption a 'major public safety issue'.[49]

For law enforcement, one of the main challenges is to technically access the data when it has the legal authority to do so. In 2017, the FBI said it required access to 7,800 devices as part of its investigations, which it was unable to access even though it had the legal authority to access the data.[50]

The argument is not only related to data stored on devices, but extends to data stored on the companies' servers. This raises another challenge related to the determining the location of the data, and reducing the time required to access information under the Mutual Legal Assistance Treaty system.

In 2018, it is very likely that governments will increase pressure on Internet companies to provide backdoor access to users' data or reduce levels of encryption mainly in dealing with major terrorist risks as it was suggested by 'Five Eyes' countries Joint Communique in 2017.[51]

The Internet industry will try to resist. Users' data is their main commodity, and losing users' trust may endanger their business model (*Figure 1*). In addition, there is a trend to recognise that the right to encrypt may be a derivative right of the basic human rights to privacy and freedom of expression.[52] Not all companies will try to resist, however: after Blackberry said it was ready to break its own encryption, other companies may also take this approach which can render them less popular with users.

The main concern for the Internet industry is ad hoc requests from governments to get access to users' data. This situation drove Google to propose a new legal framework aimed at helping foreign governments obtain digital evidence in a simpler and more organised way, and to make the process faster, unlike the MLAT system.[53] The proposal is expected to regain attention in 2018, as the concerns from governments increase. It remains to be seen whether the proposal, and other solutions which may be proposed, will carry enough safeguards and protection for users rights. This proactive trend of the Internet industry for finding efficient and legal arrangements for sharing data will also continue.

10. ICANN: Online identities, jurisdiction, and governance

Last year was a rather quiet year for ICANN. It is a continuation of the trend that started with the completion of the IANA stewardship transition on 1 October 2016. While the surface appears calm, the underlying tensions remain around three main issues which may resurface in 2018: online identity politics, jurisdiction, and data protection.

Online identities

ICANN deals with the question of online identities (as reflected in top-level domains – TLDs), which is likely to remain a controversial policy issue. The current trend in politics on focusing on identities and symbolism will inevitably impact the Internet and ultimately ICANN. The .amazon case is one example of the difficult role that ICANN has to play in tackling issues of online identities.

In 2014, the ICANN Board decided to reject the application for .amazon, submitted by the Internet company Amazon, owner of the trademark Amazon. The decision was based on advice from the Governmental Advisory Committee (GAC), which objected to .amazon being delegated to the company. The objection relied on the view of countries of the Amazon River Basin, which have been arguing that the name and domain 'Amazon' belongs to people and countries of the Amazon region.

On 11 July 2017, an Independent Review Panel (IRP) recommended that the ICANN Board re-evaluate the application for .amazon, and suggested that the Board 'makes an objective and independent judgement regarding whether there are, in fact, well-founded, merits-based public policy reasons for denying Amazon's applications'.[54] In November, a Board resolution asked the GAC whether it had any new or additional information regarding its previous advice that the applications for .amazon should not proceed.[55] This resolution raised concerns among several GAC members, and it remains to be seen how the Committee as a whole responds to the Board's request.

The ICANN Board's decision in 2018 with regard to the IRP recommendation will be one of the major 'stress tests' of the new ICANN governance architecture. And the ongoing debate will likely lead to an intensification of the discussions on several sensitive issues, such as the protection of geographical names and the relations between the GAC and the ICANN Board and the rest of the ICANN community.

Jurisdiction

After the completion of the IANA stewardship transition, ICANN's jurisdiction remained a topic of discussion, and has been one of the issues tackled in the framework of the so-called Work Stream 2 of the Cross Working Group on ICANN Accountability (CCWG-Accountability). In 2017, the discussion on jurisdiction within the dedicated sub-group of CCWG-Accountability reached a dead-end on two main issues: relocating ICANN from California to a new jurisdiction, or providing ICANN with total/partial immunity from US jurisdiction. As tthe sub-group was unable to reach consensus on these two issues, its November 2017 recommendations focused on other, less-controversial topics, related to ICANN's relations with registries and registrars based in countries affected by US government sanctions, and provisions on choice of laws and choice of arbitration in ICANN's agreements with registries and registrars.[56] But the group also recommended that 'a further other multistakeholder process of some kind should be considered to allow for further consideration, and potentially resolution' of remaining concerns.[57]

While it is unlikely that there will be any major discussions or decision on the issue of ICANN's jurisdiction (i.e., its location in the USA), we might see more focused discussion on the topic of limited, partial, relative, or tailored immunity for ICANN. Maybe in the framework of a new multistakeholder working group, as suggested in the report mentioned above.

Data protection

Ahead of 25 May, when the EU's GDPR will enter into force, ICANN has to adjust data protection to the GDPR's requirements. Specifically, ICANN will have to amend data provisions in registry and registrar framework agreements. GDPR provisions have to be observed whenever a domain is registered by European citizens, even if it is done out of the EU.

The main challenge is how to protect data of European citizens in accordance with GDPR whenever they register new domains with registrars worldwide. Data protection will also feature in the revision of the WHOIS policy (the so-called Next-Generation gTLD Registration Directory Services) and the review of the new gTLD programme are also expected to be in focus this year.[58]

Upcoming main events

The 10 trends listed for 2018 relate to 43 digital policy issues addressed by numerous actors in hundreds of events.

Each of the 43 policy issues has its own ecosystem with its own actors, language, and specific professional culture. Some policy issues such as cybersecurity are further diversifying with a focus on national security, protection of critical infrastructure, and anti-terrorism, to name a few.

The most comprehensive approach to both the 10 trends and the 43 issues will be at the following main events.

The World Economic Forum (Davos, Switzerland, 23-26 January) will address cybersecurity, artificial intelligence and other digital policy issues.

The WSIS Forum (Geneva, Switzerland, 19–23 March) will have a predominant development focus, building the agenda around the main WSIS action lines (access, health, education, etc.).

The UNCTAD E-Commerce week (Geneva, Switzerland, 16–20 April) will place particular emphasis on the role of digital platforms, a key feature of the evolving digital economy.

The Commission on Science and Technology for Development (Geneva, 14-18 May) will discuss the outcome of the work of the Working Group on Enhanced Cooperation (WGEC), which may result in proposals regarding how to guide future developments in digital policy at the international level.

The ITU Plenipotentiary (Dubai, UAE, 29 October–16 November) is likely to address some of the following contentious issues: cybersecurity, regulation of OTTs, Internet identifiers, and the future of the International Telecommunication Regulations.

The WTO Public Forum (Geneva, Switzerland; TBA) is likely to bring into focus various digital aspects that can affect digital trade (cybersecurity, standardisation, human rights, jurisdiction).

The World Internet Conference (Wuzhen, China; TBA) has a broad agenda with the main focus on linking Chinese and global digital policy players.

The Internet Governance Forum (TBA) will conclude an intensive digital policy year with comprehensive and interdisciplinary coverage of digital policy issues at more than 150 workshops and events.

In 2018, the *GIP Digital Watch* observatory (dig.watch) will provide comprehensive coverage of these and other major events.

Endnotes

[1] Geneva Internet Platform (2018) *Briefings on Internet governance and digital policy.* Available at https://dig.watch/briefings (accessed 10 January 2018).

[2] *The Economist* (2017) The world's most valuable resource is no longer oil, but data, 6 May. Available at https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-anti-trust-rules-worlds-most-valuable-resource (accessed 10 January 2018).

[3] Geneva Internet Platform (2018) *IGF Report. Final report from the 12th Internet Governance Forum*. Available at https://dig.watch/sites/default/files/IGF2017Report.pdf (accessed 10 January 2018).

[4] Castillo M (2018) Mark Zuckerberg's personal challenge for 2018: Fix Facebook. *CNBC*, 4 January. Available at https://www.cnbc.com/2018/01/04/mark-zuckerbergs-personal-challenge-for-2018-fix-facebook.html (accessed 10 January 2018).

[5] Geneva Internet Platform (2018) *WannaCry: The ransomware cyber attack explained*. Available at https://dig.watch/trends/wannacry (accessed 10 January 2018).

[6] Geneva Internet Platform (2018) *Trends in cyber-armament*. Available at https://dig.watch/processes/unge#Armament (accessed 10 January 2018).

[7] Geneva Internet Platform (2018) *Trends in cyber-armament*. Available at https://dig.watch/processes/unge#Armament (accessed 10 January 2018).

[8] Rutkowski A (2018) China's pursuit of public international cybersecurity law leadership. *CircleID*, 8 January. Available at http://www.circleid.com/posts/20180108_china_pursuit_of_public_international_cybersecurity_law_leadership/ (accessed 10 January 2018).

[9] ETSI (2018) *Network functions virtualisation*. Available at https://portal.etsi.org/TBSiteMap/NFV/NFVMembership.aspx (accessed 10 January 2018).

[10] Borg Psaila S (2012) Webinar digest: Developments and outcomes of WCIT12. *DiploFoundation blog*, 30 December. Available at https://www.diplomacy.edu/blog/webinar-digest-developments-and-outcomes-wcit12 (accessed 10 January 2018).

[11] United Nations Office for Outer Space Affairs (2018) *Committee on the Peaceful Uses of Outer Space*. Available at http://www.unoosa.org/oosa/en/ourwork/copuos/index.html (accessed 10 January 2018).

[12] Radunovic V (2017) *Towards a secure cyberspace via regional co-operation. Overview of the main diplomatic instruments*. Geneva: DiploFoundation and Geneva Internet Platform. Availale at https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf (accessed 10 January 2018).

[13] Kurbalija J (2017) Digital Geneva Convention: multilateral treaty, multistakeholder implementation. *DiploFoundation blog*, 23 February. Available at https://www.diplomacy.edu/blog/digital-geneva-convention (accessed 10 January 2018).

[14] Google (no date) *Digital security and due process. Modernizing cross-border government access standards for the cloud era*. Available at https://blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf (accessed 10 January 2018).

[15] Global Commission on the Stability of Cyberspace [GCSC] (2017) *Call to protect the public core of the Internet*. Available at https://cyberstability.org/research/call-to-protect/ (accessed 10 January 2018).

[16] The White House (2017) *Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017*. Available at https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (accessed 10 January 2018).

[17] Council of Europe (2018) *Chart of signatures and ratifications of Treaty 185*. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=gUz7n173 (accessed 10 January 2018).

[18] Kurbalija J (2017) Digital politics in 2017: Unsettled weather, stormy at times, with sunny spells. *DiploFoundation blog*, 10 January. Available at https://www.diplomacy.edu/blog/digital-politics-2017-unsettled-weather-stormy-times-sunny-spells (accessed 10 January 2018).

[19] Geneva Internet Platform (2017) *WTO Ministerial Conference 2017*. Available at https://dig.watch/events/wto-ministerial-conference-2017 (accessed 10 January 2018). WTO (1998) *Work programme on electronic commerce*. Available at https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm (accessed 10 January 2018).

[20] WTO (2017) *New initiatives on electronic commerce, investment facilitation and MSMEs*. Available at https://www.wto.org/english/news_e/news17_e/minis_13dec17_e.htm (accessed 10 January 2018).

[21] UNCTAD (2017) *Information economy report 2017. Digitization, trade and development*. Available at http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf (accessed 10 January 2018).

[22] ILO (2017) *Inception Report for the Global Commission on the Future of Work*. Available at http://www.ilo.org/wcmsp5/groups/public/---dgreports/---cabinet/documents/publication/wcms_591502.pdf (accessed 10 January 2018).

[23] Kurbalija J (2017) Digital politics in 2017: Unsettled weather, stormy at times, with sunny spells. *DiploFoundation blog*, 10 January. Available at https://www.diplomacy.edu/blog/digital-politics-2017-unsettled-weather-stormy-times-sunny-spells (accessed 10 January 2018).

[24] Geneva Internet Platform (no date) *Mapping Uber: A database of court cases and rulings*. Available at https://dig.watch/trends/uber (accessed 10 January 2018).

[25] Geneva Internet Platform (no date) *Mapping Uber: A database of court cases and rulings*. Available at https://dig.watch/trends/uber (accessed 10 January 2018).

[26] Nasralla S (2017) *Austrian court rules Facebook must delete 'hate postings'*. Reuters, 8 May. Available at https://www.reuters.com/article/facebook-austria/austrian-court-rules-facebook-must-delete-hate-postings-idUSL8N1IA21C (accessed 10 January 2018).

[27] Geneva Internet Platform (2015) *Google on content restrictions*. Available at https://dig.watch/updates/google-content-restrictions (accessed 10 January 2018). Geneva Internet Platform (2016) *Google appeals against Canadian court decision to censor search results*. Available at https://dig.watch/updates/google-appeals-against-canadian-court-decision-censor-search-results (accessed 10 January 2018).

[28] Fleischer P (2015) *Implementing a European, not global, right to be forgotten*. Google Europe blog, 30 July. Available at https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html (accessed 10 January 2018).

[29] Supreme Court of New South Wales (2017) *X v Twitter Inc*. Available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html (accessed 10 January 2018).

[30] Cambridge University (2016) *'The best or worst thing to happen to humanity' - Stephen Hawking launches Centre for the Future of Intelligence*. Available at http://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of (accessed 10 January 2018).

[31] Vincent J (2017) Elon Musk says we need to regulate AI before it becomes a danger to humanity. *The Verge*, 17 July. Available at https://www.theverge.com/2017/7/17/15980954/elon-musk-ai-regulation-existential-threat (accessed 10 January 2018).

[32] Teleanu S (2018) *Artificial intelligence: Policy implications, applications, and developments*. Available at https://dig.watch/trends/artificial-intelligence (accessed 10 January 2018).

[33] The Royal Society (2017) *Machine learning requires careful stewardship says Royal Society*. Available at https://royalsociety.org/news/2017/04/machine-learning-requires-careful-stewardship-says-royal-society/ (accessed 10 January 2018).

[34] Romm T (2016) Tech companies launch new AI coalition. *Politico*, 11 October. Available at https://www.politico.com/story/2016/10/tech-companies-launch-new-ai-coalition-229600 (accessed 10 January 2018).

[35] Microsoft (no date) *AI for Earth*. Available at https://www.microsoft.com/en-us/aiforearth (accessed 10 January 2018). Shum H (2017) Microsoft's role at the intersection of AI, people and society. *Official Microsoft Blog*, 12 July. Available at https://blogs.microsoft.com/blog/2017/07/12/microsofts-role-intersection-ai-people-society/ (accessed 10 January 2018).

[36] Bickert M (2017) Hard questions: How we counter terrorism. *Facebook Newsroom*, 15 June. Available at https://newsroom.fb.com/news/2017/06/how-we-counter-terrorism/ (accessed 10 January 2018).

[37] McMahan B and Ramage D (2017) Federated learning: Collaborative machine learning without centralized training data. *Google Research Blog*, 6 April. Available at https://research.googleblog.com/2017/04/federated-learning-collaborative.html (accessed 10 January 2018).

[38] Mozur P (2017) Beijing wants A.I. to be made in China by 2030. *The New York Times*, 20 July. Available at https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html?partner=rss&emc=rss (accessed 10 January 2018).

[39] Hern A (2017) Elon Musk says AI could lead to third world war. *The Guardian*, 4 September. Available at https://www.theguardian.com/technology/2017/sep/04/elon-musk-ai-third-world-war-vladimir-putin (accessed 10 January 2018).

[40] Geneva Internet Platform (no date) *Artificial intelligence: Policy implications, applications, and developments*. Available at https://dig.watch/trends/artificial-intelligence (accessed 10 January 2018).

[41] Rosen Jacobson B (2017) Lethal Autonomous Weapons Systems: Mapping the GGE Debate. *Diplo Policy Papers and Briefs*, no. 8. Available at https://www.diplomacy.edu/sites/default/files/Policy_papers_briefs_08_BRJ.pdf (accessed 10 January 2018).

[42] CoinMarketCap (2018) *Cryptocurrency market capitalizations: Bitcoin*. Available at https://coinmarketcap.com/currencies/bitcoin/ (accessed 10 January 2018).

[43] Collins (2017) Collins 2017 word of the year shortlist. *Word Lover's blog*, 2 November. Available at https://www.collinsdictionary.com/word-lovers-blog/new/collins-2017-word-of-the-year-shortlist,396,HCB.html (accessed 10 January 2018).

[44] Reuters staff (2017) Facebook, Google join drive against fake news in France. *Reuters*, 6 February. Available at https://uk.reuters.com/article/uk-france-election-facebook/facebook-google-join-drive-against-fake-news-in-france-idUKKBN15L0QW (accessed 10 January 2018).

[45] Miller J (2018) Germany votes for 50m euro social media fines. *BBC News*, 30 June. Available at http://www.bbc.co.uk/news/technology-40444354 (accessed 10 January 2018).

[46] Sumits A (2017) The Internet is closer to home than you think. *Cisco Blogs*, 8 June. Available at https://blogs.cisco.com/sp/the-internet-is-closer-to-home-than-you-think (accessed 10 January 2018).

[47] BEREC (no date) *What is covered and protected by the regulation*. Available at http://berec.europa.eu/eng/net-neutrality/regulation/ (accessed 10 January 2018).

[48] *The Economist* (2017) The world's most valuable resource is no longer oil, but data, 6 May. Available at https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-anti-trust-rules-worlds-most-valuable-resource (accessed 10 January 2018).

[49] Nakashima E (2018) FBI chief calls encryption a 'major public safety issue'. *The Washington Post*, 9 January. Available at https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html?utm_term=.68e9ae345f7c (accessed 10 January 2018).

[50] Nakashima E (2018) FBI chief calls encryption a 'major public safety issue'. *The Washington Post*, 9 January. Available at https://www.washingtonpost.com/world/national-security/fbi-chief-calls-encryption-a-major-public-safety-issue/2018/01/09/29a04166-f555-11e7-b34a-b85626af34ef_story.html?utm_term=.68e9ae345f7c (accessed 10 January 2018).

[51] Five Country Ministerial (2017) *Joint Communique*. Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf (accessed 10 January 2018).

[52] Kaye D (2015) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32 (accessed 10 January 2018).

[53] Google (no date) *Digital security and due process. Modernizing cross-border government access standards for the cloud era*. Available at https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi7-82fotPYAhVoI8AKHSm-8COoQFggnMAA&url=https%3A%2F%2Fblog.google%2Fdocuments%2F2%2FCrossBorderLawEnforcementRequestsWhitePaper_2.pdf&usg=AOvVaw-3juJFy-grE69Jh (accessed 10 January 2018).

[54] ICANN (2017). *International Centre for Dispute Resolution. Independent Review Process between Amazon EU S.A.R.L and ICANN*. Available at https://www.icann.org/en/system/files/files/irp-amazon-final-declaration-11jul17-en.pdf (accessed 10 January 2018).

[55] ICANN (2017) *Approved Board Resolutions. Regular Meeting of the ICANN Board*. Available at https://www.icann.org/resources/board-material/resolutions-2017-10-29-en#2.a (accessed 10 January 2018).

[56] ICANN (2017) *CCWG-Accountability WS2 Jurisdiction Subgroup. Recommendations November 2017*. Available at https://community.icann.org/display/WEIA/Jurisdiction?preview=/59643282/74581507/CCWG-Accountability-WS2-Jurisdiction-Final%20DraftFinalPDF.pdf (accessed 10 January 2018).

[57] ICANN (2017) *CCWG-Accountability WS2 Jurisdiction Subgroup. Recommendations November 2017*. Available at https://community.icann.org/display/WEIA/Jurisdiction?preview=/59643282/74581507/CCWG-Accountability-WS2-Jurisdiction-Final%20DraftFinalPDF.pdf (accessed 10 January 2018).

[58] ICANN (2018) *Next-Generation gTLD Registration Directory Services to Replace WHOIS*. Available at https://community.icann.org/display/gTLDRDS/Next-Generation+gTLD+Registration+Directory+Services+to+Replace+Whois (accessed 10 January 2018).

Author

Jovan Kurbalija

Dr Jovan Kurbalija is the Founding Director of DiploFoundation and the Head of the Geneva Internet Platform. A former diplomat, Dr Kurbalija has a professional and academic background in international law, diplomacy, and information technology.

His book, *An Introduction to Internet Governance* (**www.diplomacy.edu/igbook**), has been translated into 9 languages and is used as a textbook for academic courses worldwide.

Read more about the author: **www.diplomacy.edu/kurbalija**

We look forward to your comments – please e-mail them to
jovank@diplomacy.edu

Diplo's policy papers and briefs can be downloaded from
www.diplomacy.edu/policybriefs

If you are interested in publishing a policy paper or brief with us, please get in touch with Katharina Höne, at **katharinah@diplomacy.edu**

Please cite as: Kurbalija, J (2018) A tipping point for the Internet: 10 predictions for 2018. DiploFoundation Policy Papers and Briefs 9. Available at
https://www.diplomacy.edu/sites/default/files/Policy_papers_briefs_09_JK.pdf

The author thanks the following people for their comments on the draft:

Stephanie Borg Psaila
Arvin Kamberi
Richard Hill
Katharina Höne
Tereza Horejsova
Marilia Maciel
Adriana Minović
Virginia Paque
Ian Peter
Roxana Radu
Vladimir Radunović
Barbara Rosen Jacobson
Daniel Sepulveda
Sorina Teleanu

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


DiPLO
www.diplomacy.edu