Digital politics in 2017: Unsettled weather, stormy at times, with sunny spells

diplomacy.edu/blog/digital-politics-2017-unsettled-weather-stormy-times-sunny-spells

Jovan Kurbalija

> *...the coming year may well be remembered as a turning point in US and world history.*
>
> *Joseph Stiglitz*

Joseph Stiglitz's prediction applies to the digital realm as well. The political and economic turbulence ahead of us in 2017 will lead to *unsettled weather*. Crises will cause *occasional storms*, including the risk of major disruptions to the Internet. However, the change and turbulence will bring some *sunny spells*, too. Crisis opens new possibilities.

The forecast for 2017 starts with an analysis of the general backdrop for digital policy in 2017: the broad conceptual references for understanding the specific digital policy developments. A prediction of ten main digital policy developments for 2017 follows in the second part.

This analysis draws on continuous monitoring of digital policy carried out through the *GIP Digital Watch* observatory and further discussed during the GIP's monthly webinars. Throughout the article, references are made to the report *Top digital policy developments in 2016 - A year in review*, which rounds up the main developments for 2016.

The 2017 forecast aims to trigger discussion. Are there any other developments that you think may be important in 2017? What are your predictions? Post your comments below. Our reflections will continue here and on the *GIP Digital Watch observatory* throughout the month, culminating on 31 January with our first GIP briefing of the year. Register to join.

A. Backdrop for digital policy in 2017

Digital policy will be influenced by the challenge of synchronising the fast pace of digital developments with the much slower societal adjustments to technology-driven disruptions.

Digital growth is expected to further accelerate, mainly due to the new interplay between artificial intelligence (AI), the Internet of Things (IoT), and big data. These three technological fields are behind driverless cars, robots, and many other smart devices, such as those recently displayed at the Consumer Electronics Show in Las Vegas, USA (5–8 January 2017).

According to Nissan's CEO Carlos Ghosn, in the next 10 years we will see more techno-driven disruption than in the last 50.

Accelerated digital growth will further test the techno-absorption capacity of modern society. In 2017, this test will play out in three main fields: the Internet and the crisis of globalisation, digital developments and jobs, and the social impact of the Internet.

The Internet and the crisis of globalisation

The crisis of globalisation can been seen from statistical data (slower growth in global trade than in economic

development), public perception, and the increasing use of the term globalisation in a negative context. The crisis of globalisation will have an unavoidable impact on the Internet, which is the communications infrastructure of the global economy and society.

Over the last two decades, globalisation and the growth of the Internet have been closely interrelated. Looking ahead, if the crisis of globalisation leads to further restrictions in the movement of people, capital, and goods across national borders, the same is likely to happen with Internet traffic.

A less integrated global society would lead towards a more fragmented Internet along national and commercial borders. The fragmentation of the Internet would affect many segments of society, from business production processes that rely on an integrated Internet, to families that use Facebook, WhatsApp, and Skype to stay in touch while living in different countries and continents (refer to the World Economic Forum's 2016 report on *Internet fragmentation*).

The crisis of globalisation also brings into focus a digital realpolitik, as opposed to the more idealistic views proclaiming the unstoppable technological march towards the 'bright future of human society'. The crisis of globalisation, the tension between fragmentation and integration of the Internet, and the emergence of a digital realpolitik will influence many digital policy processes in 2017.

Digital developments and jobs

Jobs and employment, which will be high on political agendas in 2017, are directly affected by the digital economy. An increase in digital technology is often interpreted as leading to fewer available jobs.

Unemployment topped the list of What worries the world in a 2016 analysis conducted by IPSOS every month across 25 countries. Jobs were central in two major political developments in 2016: Brexit and the US presidential election. The need for better protection of jobs was one of the main drivers behind the Brexit victory. The promise of new jobs was one of the main messages in Donald Trump's presidential campaign.

In parallel to growing political relevance, digitally driven automation has been rendering millions of jobs in traditional industries obsolete. This trend continues in services and other spheres of the economy. Even jobs in call centres, facilitated by the early Internet growth, may be replaced by an advanced mix of AI and speech recognition software. This trend will be further accelerated by the fast growth of AI and robotisation.

According to the World Bank's 2016 *World Development Report*, jobs held by hotel and restaurant managers are less like to be automated, while financial professionals are most likely to be replaced by computers (Figure 1).

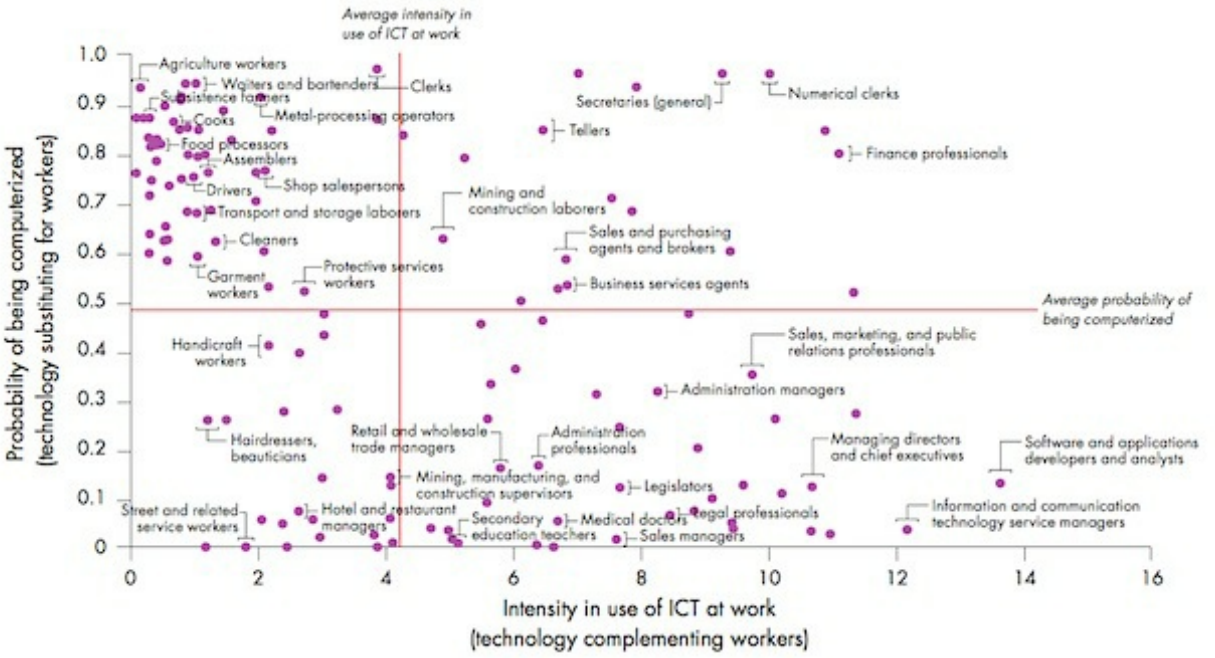

Figure 1. Interaction between technology and jobs
Source: World Bank's *2016 World Development Report*, p. 131

Different public policies to increase employment are under discussion. In the USA. For example, Trump's campaign promised major infrastructural projects which should employ more people. While such approaches may alleviate the problem temporarily, however, the structural tension between the fast disappearance of certain jobs due to technological developments, on the one hand, and the slower creation of new jobs, on the other, will remain.

In the digital era, Schumpeter's creative destruction theory is often used to describe the disappearance of old industries and jobs and the appearance of new ones. However, digital reality is different due to a longer time-lag between closing old factories and re-integrating the workforce in new economic structures.

Some analysts argue that a digitally automated society will generate fewer jobs, and the lost jobs will not be replaced. How will it be possible to replace the 47% of jobs that are likely to disappear in the USA over the next two decades, as indicated by one study from Oxford University? Discussions on guaranteed minimum income have started to emerge, to deal with the potential of permanent unemployment. Finnish experiments with basic income scheme for randomly selected 2000 Finns. Similar initiatives are expected in 2017 and the coming years.

In 2017, the digital industry, as the main beneficiary of the new economy, will increasingly come under pressure to contribute to solving the social costs of fast digital developments. Stable societies with high social capital (e.g. educated population, social cohesion) are vital to the Internet industry, which depends more on social capital than, for example, oil or extraction industries.

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. In 2017, a first constructive step could be for the Internet industry to reduce tax-withholding practices and make more robust investment in public and social projects worldwide. The implementation of the UN sustainable development goals (SDGs) provides a wider context for such a contribution of the Internet industry.

The social impact of the Internet

The adage that the Internet changes the way we live, work, and entertain has become a daily reality. Gadgets

are evolving from interesting to essential devices, affecting our daily routines and deeper cultural patterns.

For example, driverless car will not only automate our physical moves from one location to another, but also change important parts of our culture built around the use of traditional cars. Cars have been a symbol of freedom, privacy, and emancipation for years. It remains to be seen how the driverless car will affect the deeper layers of our personal and cultural upbringing. Similar examples can be found with many other devices which will become 'intelligent' in the coming years.

Digital developments will also affect political elections, public policy deliberations, social cohesion, education, and entertainment. The list goes on. While the social impact of the Internet is often framed negatively, we should keep in mind the old saying that technology is neither good nor bad nor neutral.

The discussion on the social impact of the Internet has to be carefully framed. While our goal may be to address the negative aspects (reduction of social cohesion and solidarity, less critical thinking), we may end up undermining numerous positive developments.

B. Ten main digital policy predictions for 2017

From the general backdrop – globalisation, jobs, impact – we move to ten specific trends that are likely to shape digital politics in 2017.

1. Cyber geopolitics: between conflict and cooperation

The main developments in 2016:

The cyber-driven tension between the USA and Russia marked the end of 2016 and the beginning of this year. Cybersecurity within the premier league of global politics will feature prominently on the agendas of G7, G20, and other high-level summits in 2017.

The main question will be whether the current crisis between the USA and Russia will evolve into a new cyber detente or a cold war. Some optimism can be found in the way China and the USA dealt with the crisis on economic cyber-espionage in 2015. The two countries not only resolved their bilateral tensions through dialogue, but introduced a prohibition on economic cyber-espionage in the G20 Antalya communiqué and in other policy documents.

Cybersecurity will be one of the urgent priorities for the Trump administration. In the first few months of 2017, the general contours of the future US cyber foreign policy will start emerging. During the year, we can also expect more focus on geopolitics between Russia and the USA (cybersecurity) and on geo-economics between China and the USA (digital trade, economic espionage).

In addition to national security, cybersecurity will appear in a wide range of issues, from the fight against violent extremism to ensuring the personal security of Internet users who are increasingly exposed to cybercrime and other Internet misuses.

There will be increasing recognition of externalities of lack of security and information asymmetry regarding security, possibility leading to calls for voluntary or mandatory minimum security standards, in particular of IoT devices.

In 2017, the cybersecurity discussion will follow a maturing trend that started in 2016, by shifting from mainly sensational media coverage of cyber-attacks to in-depth discussions on the vulnerabilities of modern society and the possible ways to overcome cybersecurity risks.

In 2016, NATO declared cyberspace as its fourth military operation domain. G20 leaders addressed the issue of economic espionage. Many regional organisations put cybersecurity on the policy agenda. The OSCE

introduced a second set of cybersecurity confidence-building measures. Over 30 cyber bilateral agreements were signed in 2016 (map of agreements). The United Nations Group of Governmental Experts (UN GGE) started its fifth round of discussion. For the first time, the group is composed of 25 members.

In September 2017, the UN GGE will present its report at the 72nd UN General Assembly. It is likely to address the following issues, among others t: What will replace the UN GGE and become a more permanent mechanism for dealing with global cybersecurity? How can the cybersecurity discussion be made more inclusive beyond the limited number of participating states? The UN GGE report should connect cybersecurity discussions to other non-security issues, such as technological solutions, economic development, and the protection of human rights.

In November 2017, The Global Conference on Cyberspace will be held in Hyderabad, India. It will address cybersecurity issues in a comprehensive way.

Cybersecurity will be on the agenda of at least three high-level events:

Future updates: Events | Cybersecurity | UN GGE

2. Encryption: security and privacy

The main developments in 2016:

- *Apple/FBI case brings privacy, security, encryption, and surveillance into sharper focus*
- *Tech companies enhance encryption for users*

Last year's Apple/FBI controversy gave rise to many dilemmas surrounding, on the one hand, privacy and users' rights, and on the other hand, security and the authorities' responsibility for the safety of citizens. The FBI's request for Apple to assist in unlocking the iPhone of one of the San Bernardino's terrorist attackers was not an isolated case.

Although last year's case was ultimately resolved, the main dilemmas are likely to resurface again this year, given that the industry is likely to continue to be asked to assist in dealing with cybersecurity matters. Sooner or later, stakeholders will need to make tough decisions and find a way to reach compromise. Diplo's Socratic-style script addresses the complexity of the security versus privacy dilemma, with governments, Internet users, and the Internet industry each having valid arguments for their positions on this issue.

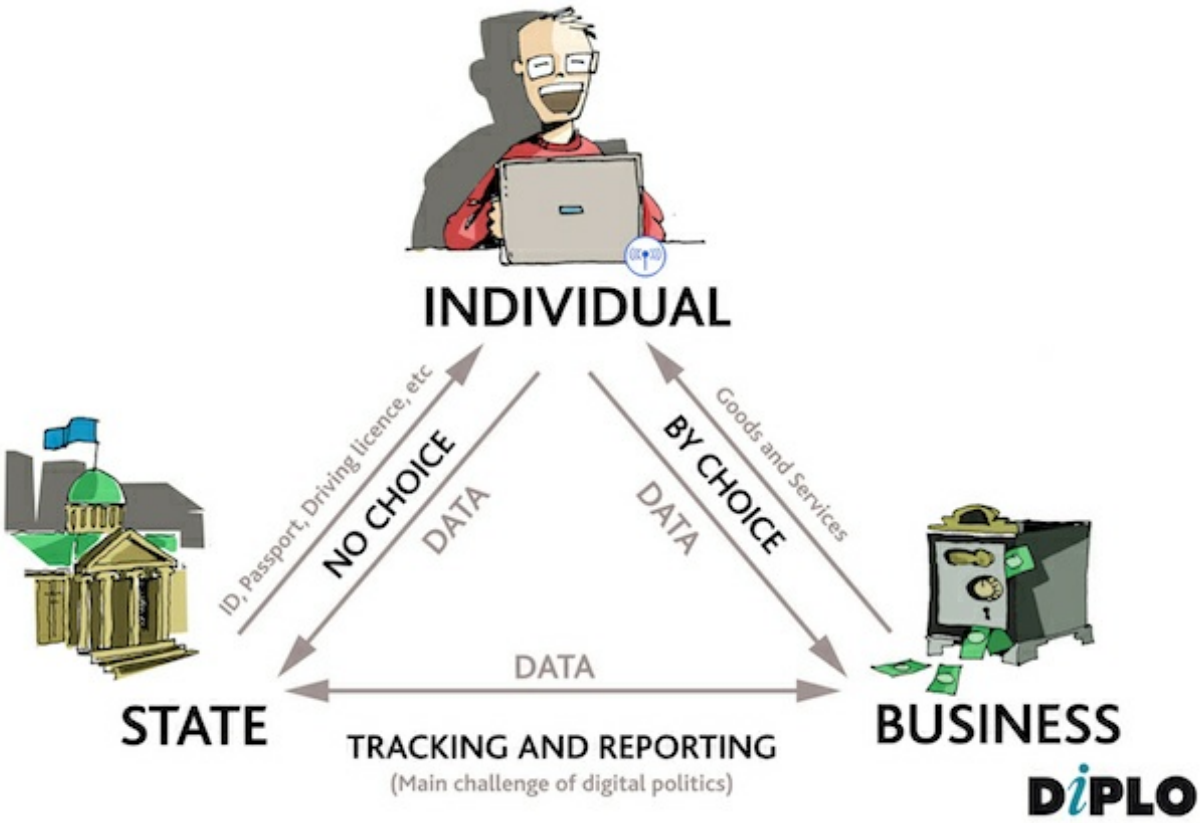

Figure 2. Data interplay

The main players in the encryption controversy are users, governments, and Internet companies (Figure 2). Driven by security considerations, governments are likely to increase pressure on Internet companies to provide backdoor access to users' data or reduce levels of encryption. Pressure will come not only from US authorities, but also from other governments worldwide. The Internet industry will try to resist. Users' data is their main commodity, and losing users' trust may endanger their business model (Figure 3). In addition, there is an increasing trend to recognise that the right to encrypt may be a derivative right of the basic human rights to privacy and freedom of expression.

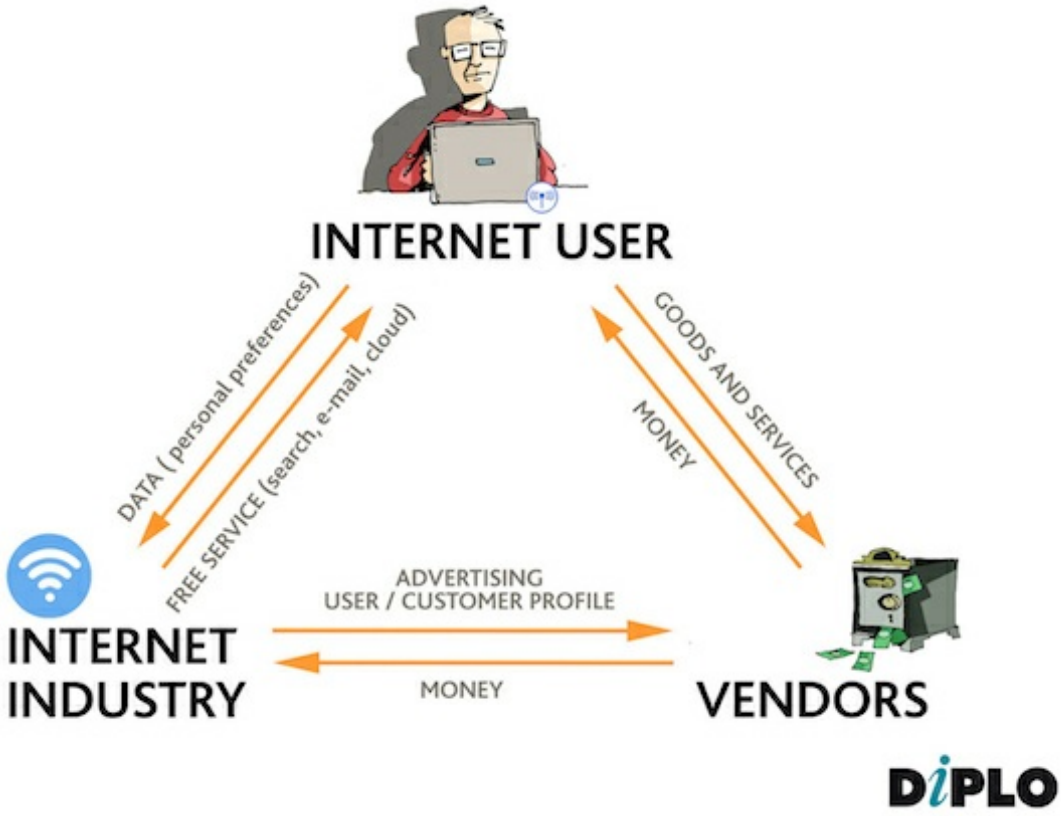

Figure 3. Internet business model

In 2017, the Internet industry will also try to avoid ad hoc solutions and aim for more predictable and formal arrangements. Since the current lack of rules is not favourable for Internet companies, new governance arrangements could provide them with more predictable and formalised ways of handling government requests for access to users' data. Such a move would not be in line with the typical business approach of minimising regulations, in particular international ones.

Public-private partnership could be a compromise arrangement which would ensure the protection of public interest in cybersecurity matters and avoid heavy regulatory pressure on the Internet industry. A potential inspiration could be found in the Montreux process, a public-private partnership aimed at providing international governance of private military and security companies.

The Montreux process construct consists of the Montreux document (2008) signed so far by 54 states, and the International Code of Conduct for Private Security Providers (ICoC), a multistakeholder initiative including governments, the private sector, and civil society. The main achievement of ICoC-a is ensuring that the private sector observes international humanitarian law (Geneva conventions) and human rights instruments. The Montreux process's 'teeth' is the ICoC Association, which provides certification and monitoring of member companies and handles complaints of alleged violations of the code of conduct.

In 2017, the search for an arrangement on access to data for security reasons could lead towards a public-private framework as a compromise between, on the one hand, the current void of international regulations and, on the other hand, a possible international treaty on encryption and access to data.

Future updates: Encryption | Privacy and data protection

3. Content policy, fake news, and violent extremism content

The main developments in 2016:

- *Initiatives and measures are introduced to combat violent extremism online*
- *Fake news and filter bubbles make the headlines*

Regulating content on the Internet has been always a controversial policy with numerous human rights, political, and economic ramifications. Combating violent extremism online will remain high on the policy agenda in 2017. In addition, social media coverage of the US presidential elections brought into focus the question of 'fake news' and, ultimately, content policy of social media platforms.

The controversies start with the effort to define fake news. Dan Kennedy makes a useful distinction between fake and false news.

...fake news is content produced by sites whose sole purpose is to game Facebook's (and Google's) algorithms for profit, and is thus a worthy target of eradication efforts. False news, by contrast, is political speech, and the way we deal with falsehoods in this country is to fight it out in Justice Oliver Wendell Holmes Jr.'s marketplace of ideas, trusting that the truth will ultimately win out.

Facebook's Mark Zuckerberg also reacted cautiously:

The problems here are complex, both technically and philosophically. We believe in giving people a voice, which means erring on the side of letting people share what they want whenever possible. We need to be careful not to discourage sharing of opinions or to mistakenly restrict accurate content. We do not want to be arbiters of truth ourselves, but instead rely on our community and trusted third parties.

In 2017, the public debate is likely to centre on two potential approaches. The first is to hold Internet companies, such as Facebook and Twitter, responsible for fake news. Some proposals argue that social networks should enjoy media status, so the Internet platforms would be regulated like newspapers or TV stations. The other approach, discussed at a few IGF 2016 workshops, is to focus more on improving social media literacy, which would help Internet users to validate information and build a more solid public debate space.

Future updates: Content policy | Intermediaries

4. Powerful interplay: AI – IoT – Big data

The main developments in 2016:

- *DDoS attacks bring IoT security into focus*
- *Artificial intelligence brings new applications and growing concerns*

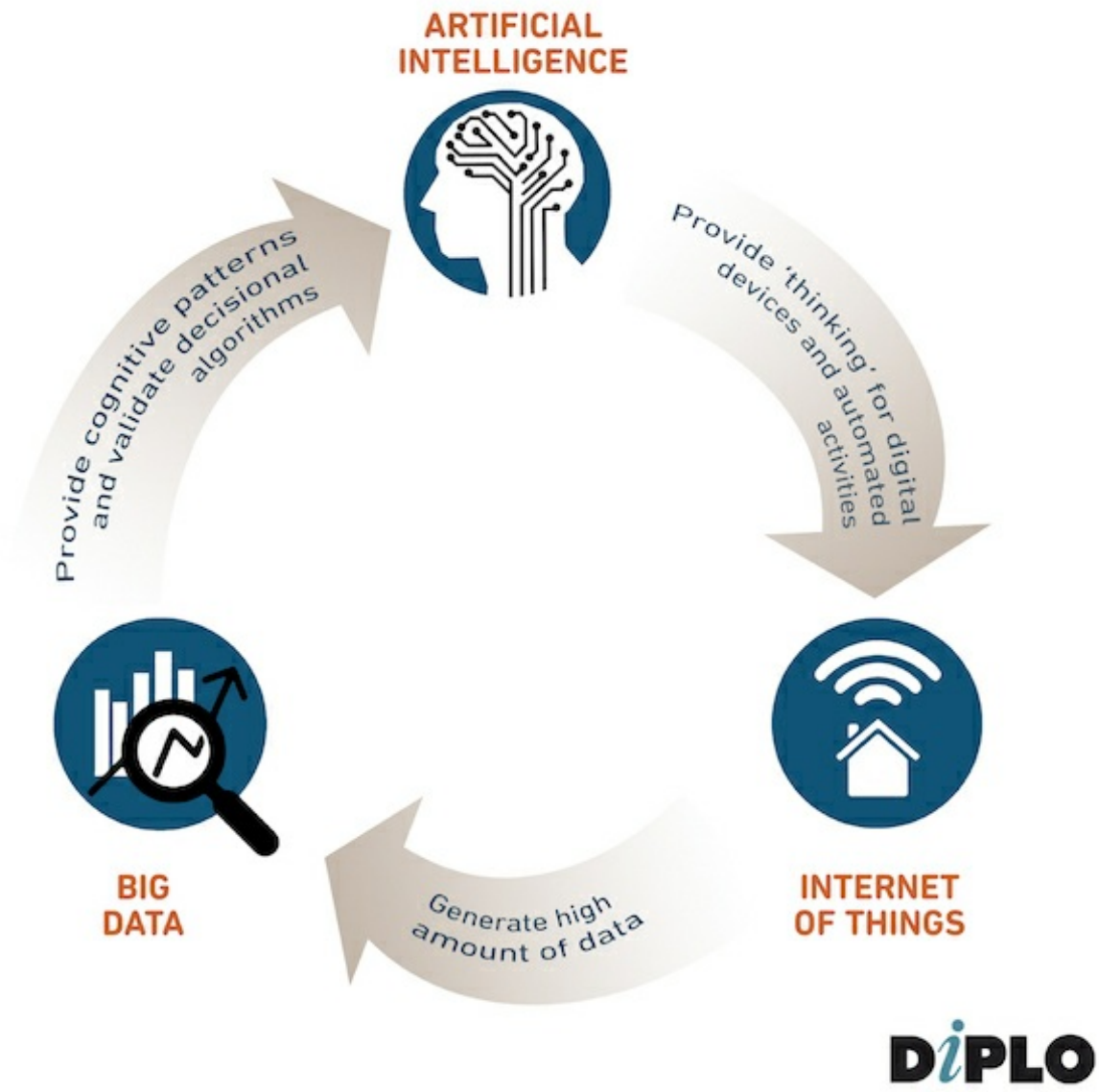

Figure 4. Interplay between Artificial Intelligence, Internet of Things and Big Data

As illustrated in Figure 4, an interplay among three technology sectors – AI, IoT, and big data – is likely to be further strengthened in 2017.

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. As demonstrated at this year's Consumer Electronics Show in Las Vegas, USA (5–8 January 2017), AI will empower a wide range of tools from from vacuum cleaners to toothbrushes and even automated personal assistants.

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 new cognitive patterns that could be integrated into new AI algorithms.

Nils Lenke, a leading scientist in AI and speech recognition, describes the AI-IoT-data cycle as follows:

You need a lot of data covering all kinds of variants of speech accents, dialects, ages, gender, and different settings, different environments. But when cloud-based speech recognition came along, things got a lot better; now, as people use it, we can see that data on our servers. The right data, covering exactly what people are doing with the technology. Not what we thought people might be doing.

The power of this emerging business model is enormous, but it also brings new challenges. It led major Internet companies (IBM, Facebook, Google, Microsoft, Amazon, and DeepMind) to launch the Partnership on Artificial Intelligence initiative, aimed at addressing the privacy, security, and ethical challenges of AI, and initiating a broader societal dialogue on the ethical aspects of new digital developments.

AI, which for many years was a topic of interest mainly for researchers and tech enthusiasts, has started to attract the attention of governments. This trend will continue in 2017, as policymakers try to determine whether existing legislation and regulations can adequately tackle the implications of AI in areas such as the labour market, safety and (cyber)security, and liability and accountability, or whether new policy frameworks are needed.

In a number of cybercrime cases during the last part of 2016, IoT devices were used as instruments in coordinated, large-scale cyber-attacks. Experts also increasingly draw attention to the privacy and data protection implications of IoT devices such as smart toys and home appliances. In 2017, the security and data implications of IoT developments will be in focus for governments and industry (as already requested in the USA and planned by the EU). Possible regulatory solutions could range from standards for IoT devices to regulatory requirements for the security of digital devices.

Future updates: Privacy and data protection | Internet of Things | Convergence

5. Data governance and data localisation

The main developments in 2016:

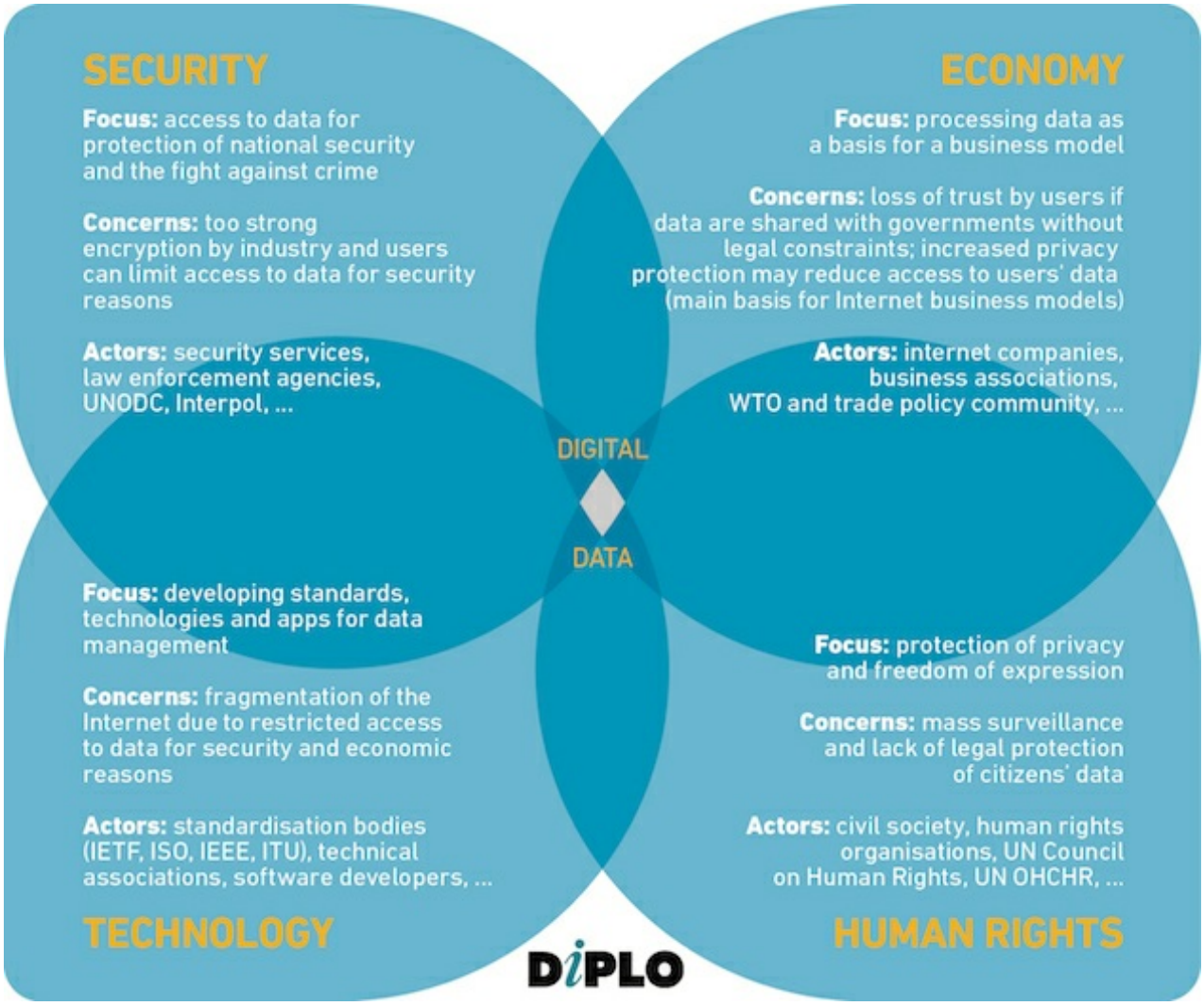

Figure 5. Interdisciplinary data governance

Data is shaping the new Internet business model. As more data is stored and processed digitally (from e-commerce transactions to health records), and often in the cloud, the governance of this data (i.e., who can collect, store, and process data, and how this can be done) becomes increasingly important. Two trends are likely to dominate data governance in 2017.

First, data governance will need to be addressed in a more comprehensive way since a solution aimed at one area may directly affect other aspects of data governance (Figure 5). For example, a policy on data in the fight against violent extremism may affect data aspects of human rights (freedom of expression and privacy). Data standards are likely to have an impact on security, economic, and human rights aspects of data governance. The use of big data in various sectors will be the main topic of discussion at the United Nations World Data Forum, to be held 15–18 January, in Cape Town, South Africa.

Second, in 2017 we can expect further pressure on data localisation (a practice which requires service providers and/or the data they store to be located within national borders). The motivations for data localisation include protectionist trade policy, national security considerations, protection of citizens' privacy, and political-driven filtering.

Data localisation will increase costs for Internet businesses, which will have to find solutions to provide services in a profitable manner, while complying with local policies.

Future updates: Privacy and data protection | Technical standards

6. Digital trade and Internet economy

The main developments in 2016:

'When trade stops, war comes' is how Jack Ma, chairman of Alibaba, China's biggest online commerce company, summarised the challenge ahead of us. Digital trade, as an engine of economic growth, could be a way to contain the protectionist wave which is expected in 2017.

As the World Bank's 2016 World Development Report indicated, the sustainable economic growth of the Internet (including digital trade) will require developing analogue policy solutions in policy areas, such as taxation, consumer protection, and labour rights.

In 2017, digital trade policy will be addressed in various fora worldwide.

For example, digital trade will be high on the agenda of the WTO Ministerial Conference, to be held on 11–14 December 2017, in Buenos Aires, Argentina. WTO negotiations face two major sets of challenges. The first is ensuring that digital trade supports the development agenda in global trade. The second is dealing with non-trade aspects of digital trade, including cybersecurity, data protection, standardisation, and online human rights. The latest China-Pakistan proposals for e-commerce have been viewed as a promising way of reaching a compromise on digital trade negotiations at the WTO.

In the EU, the digital single market is becoming one of the main engines for future integration. In 2017, it may have wider strategic relevance for the EU. Namely, if the EU manages to achieve further harmonisation in the digital field, and consolidates its internal digital market, this may help to reverse the current anti-integration tide in the EU's policy space. The fact that the EU presidency in 2017 will be held by two small but highly advanced digital countries – Malta and Estonia – could help in developing the digital single market further.

Future updates: E-commerce | Taxation | E-money and virtual currencies

7. ICANN after the IANA transition

The main developments in 2016:

- *IANA stewardship transition is completed; accountability reform continues*

For years, ICANN-related issues have been at the top of the policy agenda. This is not likely to be the case in 2017. The IANA stewardship transition from the US government to the global multistakeholder community has been successfully completed, and it is not likely to be reversed by the incoming administration.

ICANN's main focus in 2017 will be on the new generic top level domains, which will feature high on the agenda of the three public ICANN meetings to be held over the year: ICANN58, on 11–16 March in Copenhagen, Denmark; ICANN59, on 26–29 June in Johannesburg, South Africa; and ICANN60, on 28 October – 3 November in Abu Dhabi, UAE.

A potential controversy could be triggered by the question of jurisdiction of US courts over ICANN. In particular, jurisdiction could come into focus if ICANN faces many legal challenges in the US courts on issues related to rights and interests of other states and foreign entities (such as the current '.africa' court case).

Future updates: The new generic top-level domains | IANA transition and ICANN accountability | Domain Name System | Root zone

8. Digital policy shaped by court decisions

The main developments in 2016:

Numerous court rulings on digital issues confirmed our predictions for 2016:

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.

The Court of Justice of the European Union (CJEU) has already played a prominent role in the rulings on the right to be forgotten, the Safe Harbour framework, and mass surveillance.

This development is likely to accelerate in 2017 with national and regional courts filling digital policy gaps (lack of policy instruments to address policy issues).

In the first half of 2017, the CJEU is expected to issue a ruling on whether Uber should be considered a provider of transportation or a provider of information society services. This ruling will impact the evolution of the new economic model developed by Uber and other platform companies such as Airbnb. If the CJEU decides that Uber provides transportation services, the company will have to obey all rules applied to, for example, taxi companies.

In 2017, it is likely that the ruling on Microsoft by a US Appellate Court will be challenged. This landmark ruling stipulated that US authorities could not use a search warrant to force Microsoft to turn over data stored at the company's data centre in Dublin, Ireland. The ruling limits the juridical outreach of US courts over US companies with facilities abroad, an increasing practice within the Internet industry. Given the importance of the jurisdiction issue, the ultimate solution for the Microsoft case will have high relevance for future digital policy.

Courts are likely to be busy with digital issues, addressing questions of cybercrime, content removal, role of intermediaries, freedom of expression, protection of personal data, mandatory data retention requirements, and mass surveillance to name a few.

Future updates: Jurisdiction | Privacy and data protection | Convergence | Copyright

9. Connecting the dots among digital policy silos

The main developments in 2016:

- *SDGs and Internet access permeate digital policy discussions*

Policy silos are reducing the effectiveness of digital policy. As the issue of data governance (Trend 5) shows, it is difficult to have an effective policy on data without taking into consideration the technological, security, economic, and human rights aspects. The IoT – previously tackled as a technological and economic issue – received attention for its security vulnerabilities following recent cyber-attacks.

The most evident need for overcoming policy silos is in the implementation of the SDGs. The Internet as a common element for all SDGs could also play an important role in connecting the dots among various SDGs.

In 2017, many activities will focus on mapping common elements and identifying 'boundary spanners' that will create linkages between different policy silos. The CSTD Working Group on Enhanced Cooperation addresses Internet public policy issues, including how to address them in more comprehensive ways. The next meeting of the Working Group is scheduled for 26–27 January, in Geneva, Switzerland.

The interlinkages among digital policy issues and various SDGs will be one of topics at the second Multi-stakeholder Forum on Science, Technology and Innovation for the Sustainable Development Goals, on 15–16 May in New York, USA; at the WSIS Forum, on 12–16 June in Geneva, Switzerland; and at the High-Level Political Forum on Sustainable Development, on 10–19 July, also in New York, USA. The WTO Public Forum, to

be held in Geneva, Switzerland on 26–28 September, will most likely address Internet-related topics at their intersection with trade and commerce. At the end of the year, the 12th IGF meeting will feature many discussions underlining the interconnections between the various Internet governance and digital policy issues.

Future updates: SDGs and the Internet | IGF

10. Digital realpolitik: from values to interests

In 2017, the digital sphere will be affected by a global shift to realpolitik. It will inevitably bring a higher focus on interests and power considerations rather than values. In the digital realm, where values have played a vital role since the early days of the Internet, realpolitik could trigger several major consequences.

First, it may politicise issues dealing predominantly with technical aspects such as digital standards. If the issues that could be addressed by technical experts become part of realpolitik negotiations, this could restrict innovation and the future growth of technology.

Second, realpolitik may challenge the inclusiveness principle that has been introduced in the digital policy ecosystem over the past few decades, starting with Internet Engineering Task Force (IETF), and followed by ICANN and the IGF. Realpolitik is often conducted in close diplomatic circles and, sometimes, business circles with limited participation of other actors.

Third, digital realpolitik – with its shift from values to interests – may reduce the importance of human rights and common goods considerations.

Fourth, realpolitik may create a shift from global discussions towards bilateral deals and plurilateral arrangements. This trend is already noticeable in the area of cybersecurity, where the last two years saw a fast growth in bilateral agreements (Figure 6) and plurilateral arrangements (e.g. G20 economic espionage agreement). This trend could lead towards less inclusive global digital policy. Developing countries and marginalised communities worldwide would be at risk of being left out of digital policy shaping and making.

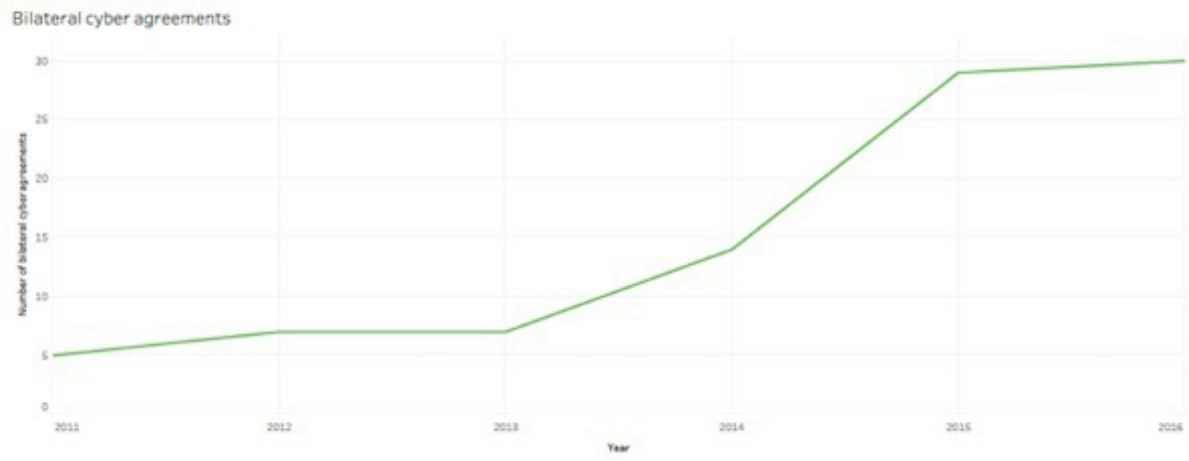

Figure 6. Rise in bilateral cyber agreements

On the positive side, realpolitik may deflate digital policy bubbles and provide a more realistic picture of interests and risks as well as winners and losers resulting from technological developments. In this way, realpolitik may contribute towards creating the basis for more solid and sustainable technological development.

C. Next steps and upcoming main events

The 10 trends listed for 2017 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 WSIS Forum (Geneva, Switzerland, 12–16 June) will have a predominant development focus, building the agenda around the main WSIS action lines (access, health, education, etc.).

The WTO Public Forum (Geneva, Switzerland, 26–28 September) is likely to bring into focus various digital aspects that can affect digital trade (cybersecurity, standardisation, human rights, jurisdiction).

The Global Conference on Cyberspace (Hyderabad, India, October) will address a broad set of digital issues through a cybersecurity perspective.

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

The Internet Governance Forum (Geneva, Switzerland, 18–21 December) will conclude an intensive digital policy year with comprehensive and interdisciplinary coverage of digital policy issues at more than 150 workshops and events.

In 2017, the GIP Digital Watch observatory will provide comprehensive coverage of these and other major events. Monthly GIP briefings on the last Tuesday in the month will provide regular updates on the progress in digital policy field. Register and join us for the next monthly briefing, on 31 January 2017.