Geneva Internet Platform
DigitalWatch

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

INTERNET AND DEVELOPMENT

The sustainable development goals (SDGs) were a frequently used concept during the series of four major digital policy events hosted in Geneva in May: the UN Commission on Science and Technology for Development (CSTD), the International Telecommunications Union (ITU) Council, the Internet Governance Forum (IGF) Open Consultations and Meeting, and the annual World Summit on the Information Society (WSIS) Forum. Digital discussions in Geneva posed some key questions: To what extent will the Internet affect each of the 17 SDGs? How will the adoption of the SDGs in September influence the key digital negotiations of the WSIS+10 Review Process in December?

More on page 3

CYBERSECURITY

Cybersecurity remained at the top of the digital agenda in May. China and Russia signed an agreement on information security cooperation, described as a 'no cyber-attack agreement'. The EU adopted an agenda on security till 2020 with cybercrime as one of three priorities (the other two are the fight against terrorism and the fight against organised crime). France passed a strict new Internet surveillance law. The USA outlined its five-points cyberstrategy principles. Some vivid academic discussions brought new concepts in the form of digital security, hybrid warfare, and comprehensive security.

More on page 4

BRIDGING POLICY SILOS

The more global digital policy intensifies, the more it compartmentalises in policy silos. Effectively addressing most digital policy issues requires bringing different policy communities to the same table. For example, discussion on access to and protection of data requires the involvement of security, trade, human and technical experts among others. This problem echoed in numerous discussions during 'Digital May' in Geneva.

More on page 7

In addition to this newsletter you can find in-depth coverage on the Digital Watch website (www.giplatform.org/digitalwatch/) and join live discussion on the last Tuesday of every month online or at the Geneva Internet Platform Premises | Digital Watch is published by the Geneva Internet Platform/DiploFoundation | Design by Viktor Mijatovic, Diplo's CreativeLab | Send your comments to digitalwatch@diplomacy.edu

CAUTIOUS PREPARATIONS FOR A BUSY AUTUMN IN DIGITAL POLICY

The month of May in digital Geneva was a prelude for acceleration of digital policy in the rest of the year. In autumn this year, the main event will be the WSIS+10 High Level Meeting (New York, 2-3 December 2015), which will address the future of the WSIS process as a general framework for digital policy and specific issues such as the extension of the IGF mandate. The globalisation of the Internet for Assigned Names and Numbers (ICANN) is another process which will mark digital policy in the autumn. On 30 September, the proposal for the globalisation of ICANN should be ready. The success in meeting this deadline or a prolongation of the process will inevitably impact broader digital policy, and the WSIS+10 negotiations in particular.

The WSIS+10 process and ICANN's transition provided a broader backdrop for Digital May in Geneva. There was a lot of signalling and preparations, in particular for the forthcoming WSIS+10 negotiations. The main events included:

4–8 May 2015

The 18th session of the CSTD had direct relevance for the WSIS +10 process. The agreement on the resolution on the role of science, technology, and innovation (STI) for development was reached quickly. More controversial was the second resolution on the WSIS follow-up. Since there was difficulty in reaching consensus on the issues such as the future of the IGF and cooperation, the CTSD retreated to the text of the 2014 resolution, making a few minor updates. Hot potatoes have been passed to negotiators in New York.

17 May 2015

The ITU celebrated 150th anniversary. Anniversaries are as much about the present and the future as they are about the past. While celebrating the ITU's long history, the digital community also had a chance to reflect on our time: what to learn from how our predecessors handled innovative technologies such as the telegraph, radio, and the telephone, to name a few. In parallel to the celebrations, the ITU Council met and discussed IG, among other issues. *See: 'ITU celebrated 150 years' on page 6.*

20–22 May 2015

The IGF's MAG met to discuss preparations for the tenth annual IGF meeting, scheduled to take place in João Pessoa, Brazil, 10-13 November 2015. The MAG evaluated 267 proposals for workshops, civil society, and the business sector in order to prepare the IGF programme. Every year, the proposals are a good indicator of the focus and priorities of the global digital community.

This year, the highest number of proposals covered the question of human rights and the Internet, while the least covered issues are legal ones (e.g. jurisdiction, responsibility). *See table: IG at a glance - What is the focus of the 2015 IGF? at page 3.*

25–29 May 2015

A busy Digital May in Geneva concluded with the WSIS, which gathered 1800 participants from 140 countries. The underlying theme was the link between digital policy and the SDGs. Digital issues were discussed in their interplay with health, agriculture, climate change, cultural and other fields where ICT impacts modern society.

Anytime you see this icon, there is more background material in the online version. Alternatively, visit www.giplatform.org/digitalwatch for more in-depth information.

IG at a Glance - What is the focus of IGF 2015?

Based upon the number of event proposals for IGF 2015

INTERNET AND THE SDGs

The main concern during May's digital events in Geneva was the lack of direct references to the Internet in the 17 SDGs. One explanation for this omission was that digital is 'tacit' and 'assumed' and touches on all SDGs. Starting from this assumption, many participants tried to map this 'tacit' SDG to the 17 actual SDGs by indicating how digital will affect health, infrastructure, trade, and other specific SDGs. The most critical view was expressed during the WSIS Forum Interactive Session on E-health and Social Media (25 May 2015):

> ...there is deep disappointment in the health community that there are no ICT-related goals among the SDGs. ICT is as relevant today as during the time of the MDGs development, and its vital role is increasingly recognized in all sectors. To argue that ICT is cross-cutting and therefore not needed in the SDGs minimizes ICT's contribution to development. It will be seen in the years to come as a fundamental omission and lack of leadership that cannot be rectified with governance forums and action lines.

This critical reflection opens real debate. The Internet is so instrumental for achieving the SDGs that any disruption or malfunction of the Internet will affect the overall development agenda. It does not need to be a technical failure (cut off internet cables, virus attack); it could also be a policy issue, as the recent discussion on 'internet.org' has vividly shown. If Internet service providers in developing countries do as Facebook did with 'internet.org' and filter access to a limited number of websites, it could affect access to the Internet in its full richness and, ultimately, affect most of the SDGs.

DEVELOPMENTS IN MAY 2015

Cybersecurity

increasing relevance

In May, the trend of 'securitisation' of digital policy continued. China and Russia signed an agreement on information security, which is being referred to as a cyber 'non-aggression' pact. The agreement is a framework document reconfirming the previous positions of the two countries towards a stronger normative framework in cybersecurity. NATO and the European Union (EU) intensified cooperation in countering 'hybrid warfare', which includes extensive use of cyber-tools. The EU adopted the European Agenda on Security (2015-2020) where the fight against cybercrime is listed among the top three priorities alongside preventing terrorism and fighting organised crime. In his speech in Seoul, US Secretary of State John Kerry outlined the US global cyber policy, and offered five cyber-stability principles:

First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.

Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.

Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.

Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.

Every country should do what it can to help states that are victimized by a cyberattack.

Global IG Architecture

same relevance

Admiral Michael Rogers, the new director of the US National Security Agency (NSA), argued in his speech at a cybersecurity conference in Tallinn, Estonia, that the Law of the Sea could inspire the development of a Law of the Internet. According to Reuters, he said: 'I'd like to see if we can create something equivalent to the maritime world in the cyber world that enables us to keep moving information, keep moving commerce, keep moving ideas on a global basis. Can we create a "global commons", so to speak, that enables open, reliable, safe and resilient communications, a flow of information and ideas?' Apart from an interesting analogy with the Law of the Sea, Rogers opened the possibility of establishing a global normative framework in cyber matters.

ICANN and IANA Transition

increasing relevance

The announcement of the departure of Fadi Chehadé, ICANN's President and CEO, in March 2016, left the Internet community speculating about a possible impact on the IANA transition, which many say will not happen by the 30 September deadline. Meanwhile, ICANN started dealing with the gTLD 'dot sucks' controversy, while registration fees remain high, and concerns about the possible misuse of this domain.

Online privacy and data protection

increasing relevance

The US House of Representatives passed the Freedom Act with the aim of reforming the NSA's powers. At the same time, US tech companies, and civil liberties and privacy activists have urged the White House to pull back efforts to weaken encryption or include law enforcement back doors in technology products.

In France, a new surveillance law has made a radical move to allow authorities to demand data from ISPs and phone companies, and to place cameras and recording devices in private homes. This has raised a lot of concern in civil society, which protested with a '24-hours before 1984' campaign, drawing a parallel to George Orwell's novel.

Net neutrality

same relevance

Net neutrality regained importance due to the newly launched Internet.org – an initiative by Facebook to connect regions that do not yet have Internet access – with the caveat that only a limited number of websites will be accessible. While Indian start-ups pulled out of the initiative, a global campaign to request Internet.org to provide access to the full Internet is under way.

In the EU, the reference to net neutrality was allegedly removed from a leaked European Council non-document, which was surprising, and goes against recent trends in the region to protect net neutrality.

E-commerce

increasing relevance

Digital Single Market plans were unveiled by the EU. The plans promise a simple functional approach of removing barriers and harmonising rules, among others.

AHEAD IN JUNE

ITU CELEBRATES 150 YEARS

Delegates at the first ITU conference in 1865 (Source: ITU)

'The farther back you can look, the farther forward you are likely to see.' Winston Churchill

On 17 May 2015, the International Telecommunication Union (ITU) celebrated its 150th anniversary. In its long history, the ITU has witnessed all main telecommunication innovations starting from the electric telegraph, which triggered the establishment of the ITU (then as the International Telegraph Union), via telephone, radio, and satellite to digital networks.

Some issues transcend eras. For example, there is not much difference in discussions on privacy and security between the ITU's St Petersburg conference in 1885 and our time. Like today, 130 years ago delegates searched for the balance between the protection of free communication and the need to protect security and public order. *see: page 7.*

A decisive moment in the ITU's history was triggered by the sinking of the Titanic, when the SOS distress call from the Titanic did not reach other ships fast enough. One of the reasons was that at the time, not all shipping companies used the same distress call (SOS). The Titanic was equipped with a Marconi radio apparatus which used the CQD distress code. In order to protect Marconi's dominant market role, this apparatus did not allow communication with Telefunken and other smaller operators.

The SS Californian, just a few miles from the Titanic, operated a Telefunken apparatus and used the SOS distress code. The SS Californian could not hear the Titanic's call for help. Just a few months after the Titanic tragedy, the ITU organised the 1912 International Radiotelegraph Conference, which, among many other issues, agreed on the use of a common wave-length for SOS signals.

In 1912, at the London Conference, the ITU laid the basis for the global radio telecommunication system that is still valid today. This year, the ITU will host the triennial World Radiocommunication Conference (2-27 November 2015) in Geneva, aimed at adapting the 1912 regime to the latest technological changes.

PÉTER MAJOR – NEW CHAIRMAN OF THE UN CSTD

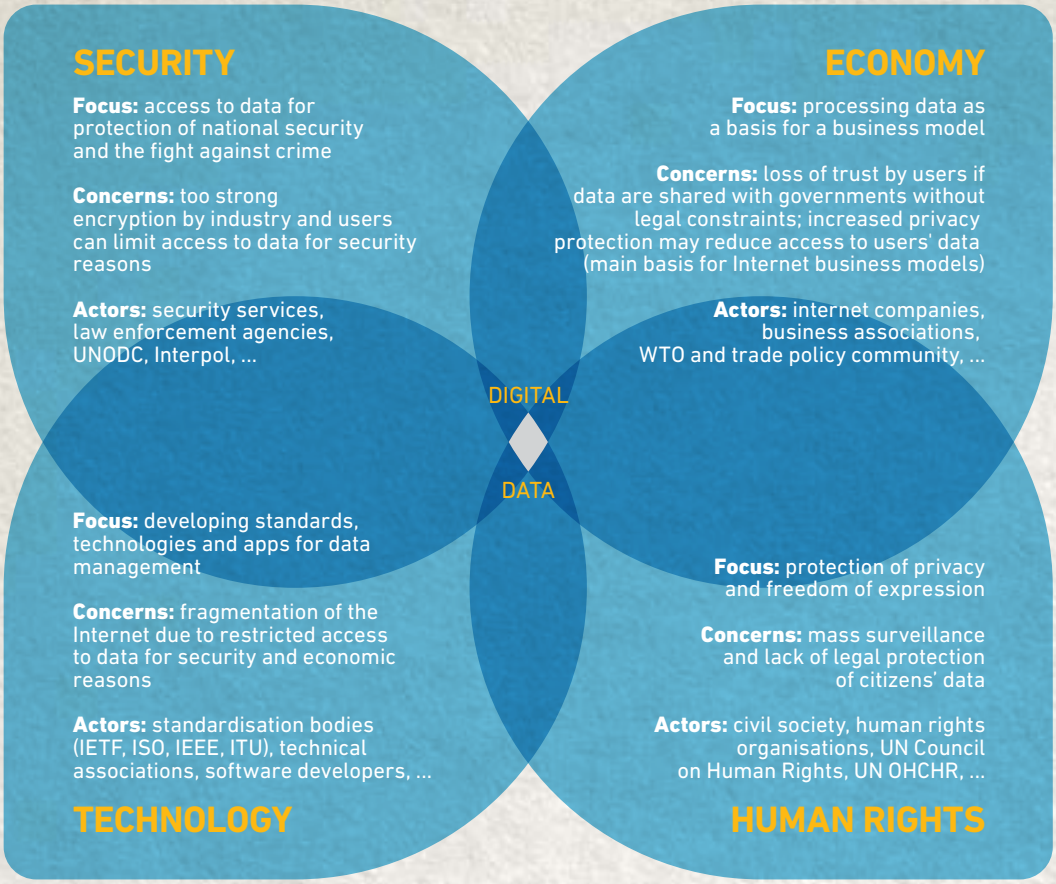
Hungarian Péter Major was elected Chairman of the UN Commission on Science and Technology for Development (CSTD) during the CSTD's May session. Major is a former ITU official and a prominent actor in global digital policy processes.

In an interview Major highlighted three main challenges converging towards the WSIS+10 High Level meeting (2-3 December 2015): how to continue the WSIS Process beyond 2015, how to link digital policy to the sustainable development goals, and how to strengthen the role of the IGF.

He expects that the CSTD's work will be shaped by the growing realisation of governments about the importance of digital policy issues. On the positive side of this development is the growing visibility and relevance of digital policy in global diplomacy. On the negative side is the potentially higher politicisation of the previously more isolated technical side of digital policy. Most bodies, including the CSTD, would have to deal with this emerging reality.

At the May meeting of the CSTD, there was a small, but important shift from the previously sharply divided policy debate to an inclination towards converging solutions. In addition, there was a 'swap' of support and criticism around specific issues (WSIS report, mapping exercise). This new dynamism should create more spaces for possible consensus and, at least, reasonable compromise. Major highlighted our responsibility to work towards sustainable global policy solutions for the future of the Internet, a great enabler of our era.

BRIDGING POLICY SILOS IN THE DIGITAL FIELD



The omnipresence of the Internet in modern society makes most digital policy issues transversal. Yet, a transversal approach is more an exception than a rule in digital policy on both national and international level. For example, data protection is rarely addressed in a holistic way from security, human rights, economic, and technical perspectives (*see illustration*). E-commerce, the fight against cybercrime, to name a few, approach as well.

Why does bridging policy silos matter? Exclusive sectoral solutions are sub-optimal. For example, if data protection standards are developed without security and human rights considerations, future data-driven applications could have in-built weaknesses. Ultimately, such solutions could impact the core values of an open and stable Internet.

Are policy silos unique for the Internet? No. Policy silos present a challenge in many policy areas. Climate change involves scientific, economic, development, and health policy communities, among others. Similar complexity exists in dealing with migration and humanitarian assistance. Geneva, as an important hub for all of these issues, should facilitate research and exchange in cross-sectoral policy coverage.

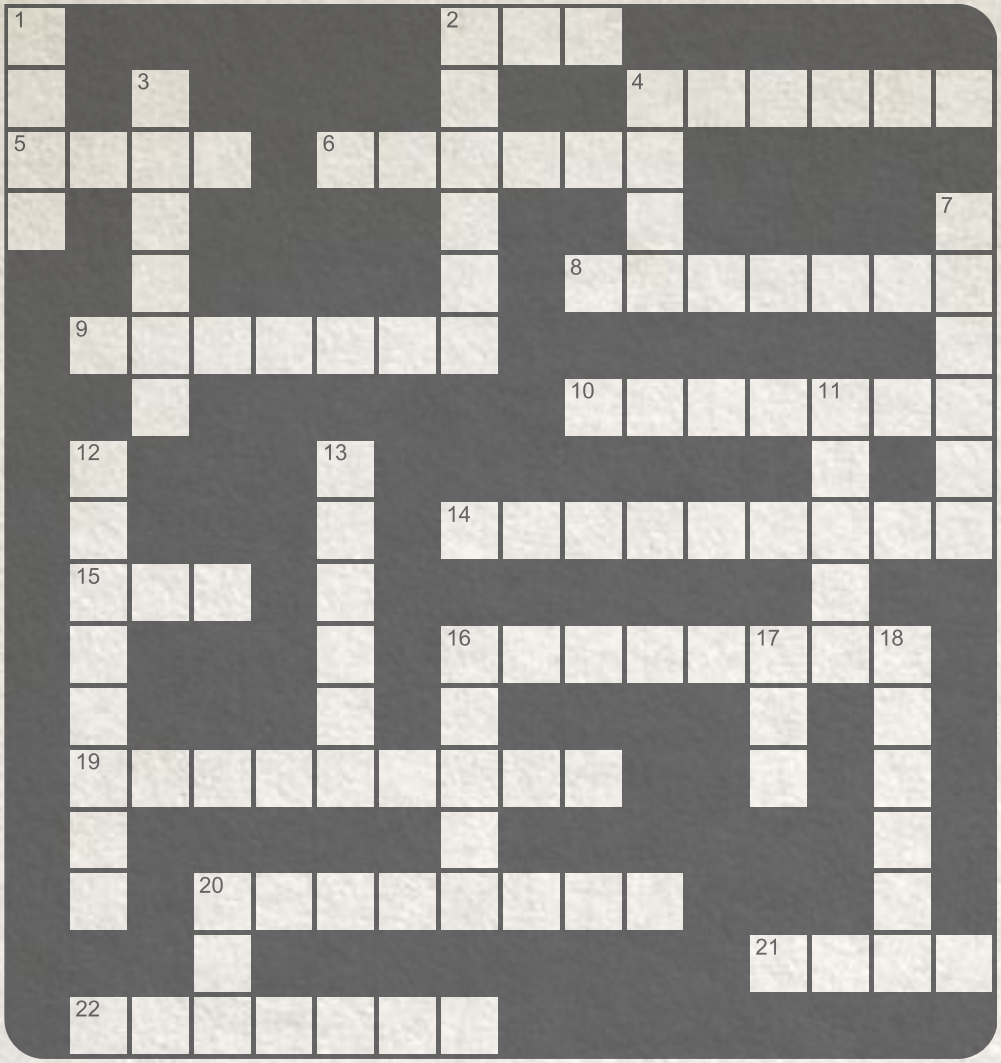
What are the limits in dealing with policy silos? Any attempt to bridge policy silos should be based on realistic expectations. Namely, we tend to work in social groups of limited size which can focus only on a limited number of policy aspects (technology, security, human rights). With time, policy communities are reinforced by the use of specific language, acquiring tacit understanding of the core concepts, and developing social and professional networks. These considerations should be taken into account for any attempt to bridge policy silos.

What can be done? An effective way of bridging policy silos is to develop a context and use smart nudging to bring different professional and institutional cultures closer together. One practical approach is to encourage the work of individuals who can span boundaries by understanding the ethos and language of various policy communities (technical, legal, security). In addition, bridging policy silos should include a focus on language. Language is both a problem, which is usually used to fortify policy silos, and a possible solution. By simplifying professional language and reducing the use of abbreviations and acronyms, we can facilitate easier cross-silo communication.

What are the next steps? Following our ongoing research and the Geneva Message (November 2014), the Geneva Internet Platform will focuses on bridging policy silos in digital policy by organising discussions with different policy communities (technical, security, human rights, economic) and facilitating training and research activities on fostering a cross-sectoral approach to digital policy.

Based on a text published by Dr Jovan Kurbalija in the Hufftington Post.

TEST YOUR CYBERSECURITY KNOWLEDGE



Across

2 The acronym of the UN expert group that has examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them (3)
4 One of the largest annual hacker conventions, held every year in Las Vegas, Nevada (6)
5 A team of experts tasked with handling computer security incidents within a critical information infrastructure, first organised at the Carnegie Mellon University in the USA (acronym) (4)
6 According to a report from the Munich Security Conference of 2015, cyberwarfare will be a component of a modern type of warfare called ___ warfare (6)
8 Name of the country which, in 2007, suffered one of the first major cyberattacks on its national e-infrastructure (7)
9 One of the leading research documents on the applicability of the interna tional law to cyber warfare - a ____ Manual (named after a European city) (7)
10 One of the most renowned hackers, the author of the book, Kevin (7)
14 An international Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, recently extended to include computer exploits (9)
15 Network system that translates computer (IP) numbers into domain names (3)
16 Type of an online scam to acquire personal information such as usernames, passwords, and credit card details (8)
19 One of the key pillars of cybersecurity (9)
20 City where 2014 Internet Governance Forum was hosted (8)
21 Unsolicited e-mail (4)
22 Name of the virus that was used for an alleged Israeli attack on computers at Iranian nuclear facilities (7)

Down

1 European security organisation increasingly focusing on cybersecurity (4)
2 Author of the science-fiction novel who coined the word 'cyberspace', William (6)
3 Type of malware which carries out loss or theft of data, bearing a name of a known Ancient Greek deception story (6)
4 Form of cyberattack involving multiple computers aimed at rendering a targeted server or network inaccessible for a period of time (acronym) (4)
7 A skilful computer user that seeks and exploits weaknesses in a computer system or computer network (6)
11 US-based organisation that manages Internet names and numbers; one of the most important players in global Internet governance (5)
12 The city of birth of the Convention on Cybercrime of Council of Europe of 2001 (also known as _____ Convention) (8)
13 A cyber-espionage campaign allegedly conducted by Chinese hackers against western corporations, dubbed Operation ___ (6)
16 The infamous surveillance programme instigated by the US NSA (5)
17 Acronym for a multistakeholder body designated by a decision of the World Summit on the Information Society (3)
18 City after which the Conventions establishing the standards of for the humanitarian treatment of war (possibly also applicable to cyberspace) were named (6)
20 The main UN agency for telecommunication issues (3)

Developed by Diplo CreativeLab

Across: 2 GGE, 4 DEFCON, 5 CERT, 6 Hybrid, 8 Estonia, 9 Tallinn, 10 Mitnick, 14 Wassenaar, 15 DNS, 16 Phishing, 19 Education, 20 Istambul, 21 Spam, 22 Stuxnet.
Down: 1 OSCE, 2 Gibson, 3 Trojan, 4 DDoS, 7 Hacker, 11 ICANN, 12 Budapest, 13 Aurora, 16 PRISM, 17 IGF, 18 Geneva, 20 ITU.