IGF Daily **No. 3** – Wednesday, 20th December, 2017

IGF DAILY

REPORTING DAILY FROM THE 12th INTERNET GOVERNANCE FORUM

dig.watch/igf2017

IGF Daily prepared by the Geneva Internet Platform with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation

HIGHLIGHTS FROM DAY 2

The second day of the 12th Internet Governance Forum was dominated by sessions on cybersecurity, content policy, and infrastructure and emerging technologies. Here we recap the main themes.

E-commerce: Will digitalisation widen existing divides or revolutionise the economy?

Digitalisation has affected many aspects of society. One of them is trade, which is increasingly conducted over the Internet.

The World Trade Organization's Ministerial Conference (MC11) which took place last week, and the related debate on e-commerce rules which had been picking up momentum for a few months already, brought development issues into discussion.

Countries which lack Internet access are at a risk of exclusion. There is no stopping digital trade from evolving, nor should there be, as long as the evolution happens through the lens of appropriate rules, regulations, and inclusion, experts warned. Policymaking at the national and international levels needs to mitigate the risk that digitalisation can widen existing divides and create new gaps.

The sharing economy (such as Uber, and AirBnb) is a recent phenomenon in the evolution of e-commerce. Some see it as an efficient model for utilising excess resources – a view which may not be shared by those who are concerned about the labour implications for contractors. A main question was how to adjust to the sharing economy, since challenges tend to arise at a faster rate than society is able to adapt to them.

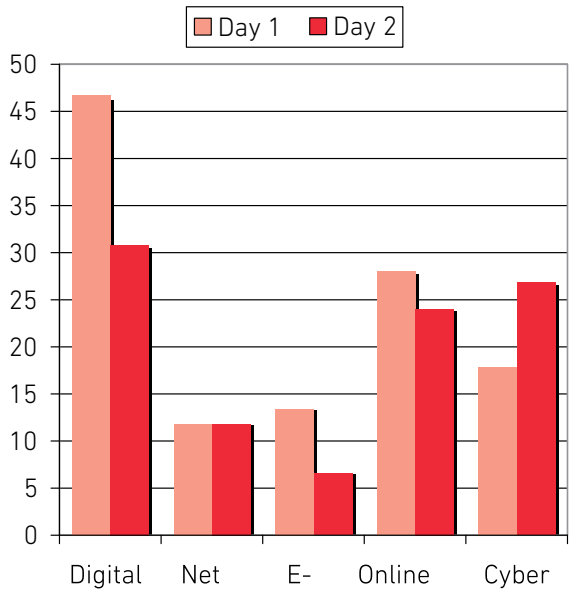
Continued on page 2

A LOOK AT THE PREFIX MONITOR

The Prefix Monitor for the second day of the IGF, based on our analysis of close to 60 transcripts, confirmed two trends and revealed a new one.

On Monday we observed that the popularity of the prefix *digital* was triggered by the growing use of the concept of digitalisation of society. The prefix was also widely used to refer to *digital* governance rather than Internet governance. The tendency to use *digital governance* continued during the second day of the IGF.

Retaining its popularity, the prefix *cyber* increased significantly in use on Day 2. This was due to the number of cybersecurity discussions yesterday, starting from a main session on global cooperation on cybersecurity, to more specific workshops. Although both the prefixes *digital* and *e-* had a lower frequency, a closer look at the transcripts confirms this year's trend for *e-* to prevail over *digital* in economic issues.



This report has been prepared by the Geneva Internet Platform, with support from the IGF Secretariat, ICANN, the Internet Society, and DiploFoundation.
Session reports and updates from the 12th Internet Governance Forum are available on the *GIP Digital Watch* observatory at dig.watch/igf2017
Click on the icon in the digital version to access links and additional information.

Continued from page 1

Telecom infrastructure: From submarine cables to the Internet of Things

Many of us take the Internet for granted, and we do not pay much attention to its underlying infrastructure. We cannot have the Internet without physical infrastructures, and the availability of such infrastructures remains a challenge in many parts of the world. One solution that is increasingly considered and implemented around the around is the deployment of community networks. These networks are developed by local communities, and this is where their value resides, but they do require support from both policy makers and operators in order to be sustainable.

Some countries are dependent on submarine cables which ensure their connectivity to the global Internet. This makes submarine cables part of the Internet's critical infrastructures, requiring adequate protection not only through measures taken by the companies that own them, but also through international agreements preventing countries from causing disruptions.

As Internet of Things (IoT) devices become ubiquitous, and companies start deploying IoT-dedicated networks, cybersecurity concerns become more and more relevant. Can regulation help address such concerns and prevent cyber incidents involving IoT devices and networks? If so, should regulation be carried out on the national or the international level? Or are these issues better addressed through standards and certification systems developed by the industry and the technical community?

Answers to these questions vary, but one thing seems to be certain: users need to be educated about cyber hygiene and what they can do when it comes to security and privacy in an IoT environment.

But cybersecurity is not the only concern when it comes to the evolution of the IoT. Inclusion should also be considered, and efforts are needed to ensure that IoT devices are accessible to persons with disabilities.

Cybersecurity: Calling for a human-centric approach

One of the main issues in cybersecurity is how to tackle the seemingly conflicting needs of authorities and users. Law enforcement agencies often need access to users' data when investigating crime; users want their rights to be safeguarded. Although Day 1 discussions supported encryption as a necessary facet of both security and privacy, encryption was described on Day 2 as often being a hindrance to national security.

Although it is often said that security and privacy are complementary (you cannot have privacy without security), some discussions referred to privacy as a possible trade-off for greater security. Rather than balancing security with

Continued on page 3

COUNTRIES ARE DEVELOPING OFFENSIVE CYBER-CAPABILITIES

Around 30 countries are developing or have developed offensive cyber-capabilities, according to a new study published on the *GIP Digital Watch* observatory, and launched yesterday. Put simply, these states would be able to conduct a cyber attack against another organisation or country in anticipation of such an attack. Referring to the study, which links to official documents and media coverage, experts yesterday called for greater transparency on the development of such cyber-capabilities.

TOWARDS A MORE TANGIBLE IGF: THE IGF 2017 GENEVA MESSAGES

As we outlined in our first newsletter on Monday, there are several innovations in this year's Internet Governance Forum. One stands out, perhaps more than others: *The IGF 2017 Geneva Messages*.

In short, these are summaries of the main points raised during the main sessions and high-level sessions held throughout the week. Their purpose is to enhance the impact of the IGF, and contribute to more visible IGF outputs – a welcome aspect for those who have been encouraging more tangible outcomes.

Of a non-binding nature, these messages are published on the IGF website and will be included in the Chair's Summary at the end of the meeting.

Curious to know what they say? Take a look!

privacy, however, experts are calling for a human-centric approach to cybersecurity, focusing on people, and not just on technology. Users need to regain control over their data; as the owners of their data, they should be the ones deciding what happens to it.

Every company that uses ICT has responsibilities – or so-called 'duties of care' in relation to cybersecurity, according to the Dutch Cybersecurity Council. Experts stressed the need to explore what standards, regulation, and self-regulatory measures, currently exist. We also need to develop a culture of cybersecurity, in which stakeholders understand what is expected of them, and what they can expect in return.

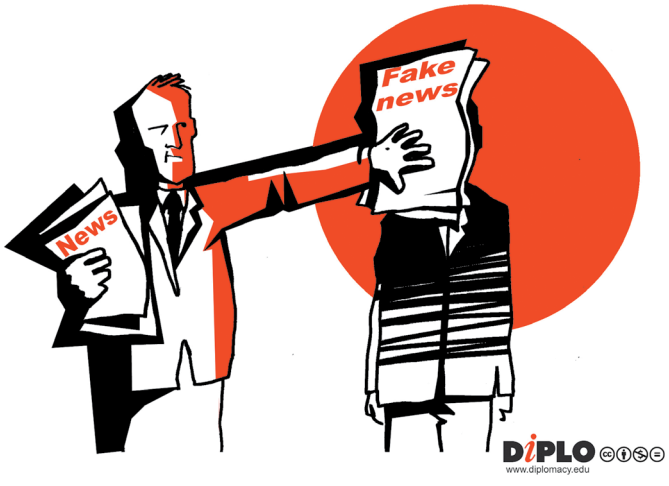
Fighting fake news, misinformation, and information disorder

If there is one thing that has caught everyone's attention, it's the issue of fake news. Gaining prominence right after the 2017 US presidential campaign, during the past few months fake news has been the subject of controversy, of tension for Internet companies, and of new studies that seek to unravel why and how this phenomenon is leading to public mistrust and manipulation of public opinion. The term has also morphed into new terms, including *misinformation*, *disinformation*, *alternative facts*, and *information disorder*.

This phenomenon is not new: every great telecommunications invention brought about an influx of propaganda. This now has an instantaneous effect due to lightning-fast digital technologies; the fact that fake news is cheap to produce (compared to high-quality news which costs money) aids its widespread and instantaneous dissemination.

When this issue surfaced, Internet companies came under fire for allowing fake news to spread on their platforms. Critics held that platforms were responsible for content that goes through their pipes. At the same time, as noted in yesterday's discussions, governments also have a responsibility to invest in education and media literacy. Media pluralism and education can be more effective in responding to fake news than simply publishing a retraction or a fact check.

The tools used to combat fake news include legal and technical means, which do not come without their fair share of challenges. From a policy perspective, one of these complexities emerges from the need to balance regulation with the promotion of freedom of expression. Solutions include developing more transparent measures (and algorithms), educating users about their information rights, and more support for technological innovation. A more daring suggestion was to tax Internet platforms that systematically propagate disinformation on a regular basis, when it has been proven that the disinformation has created a problem.



In addition to this summary, read our reports from most sessions, at dig.watch/igf2017

THE IGF AS A PROCESS: NRIs COLLABORATIVE SESSIONS, DYNAMIC COALITIONS, AND BEST PRACTICE FORUMS

Dynamic Coalition (DC) meetings and collaborative sessions organised by national and regional IGF initiatives (NRIs) continued today.

The DC on Platform Responsibility explored issues related to platform accountability and responsibilities in relation to human rights. Regulators around the world take steps to regulate online platforms, requiring them to implement content control policies, such as quickly removing online content containing hate speech or violent extremism. But the rules are not always clearly defined, and their implementation may pose challenges to human rights.

The meeting of the DC on Net Neutrality served to share regulatory practices around the world. Among them were the EU regulatory framework, which outlines net neutrality principles for states to implement at national level, and India's recently adopted recommendations noting that providers should not discriminate Internet traffic based on content, sender, receiver, protocols, or the equipment used.

Public libraries can be providers of free and open access to the Internet and online information, and this is the key message disseminated by the DC on Public Access in Libraries. Libraries can (and do) empower vulnerable communities (such as persons with disabilities and indigenous communities) to make meaningful use of the Internet.

The DC on Trade and the Internet adopted a resolution on transparency and inclusiveness in trade negotiations, outlining two principles: *transparency* – governments' responsibility to inform citizens about how they regulate trade and to receive public comments on such regulations; and *consultation* – governments' responsibility to ensure that interested stakeholders can meaningfully contribute to the drafting process.

In discussing artificial intelligence (AI) and the Internet of Things, the DC on IoT stressed that standards should cover issues such as security of and interoperability between devices and systems. The DC called for standard-setting organisations to collaborate towards more harmonised approaches.

The DC on Community Connectivity showcased the potential of community networks as bridgers of the digital divide, especially in rural areas. Such networks can also promote sustainable access, in the sense of allowing individuals not only to connect to the Internet, but also to stay connected over time.

In a collaborative session on multilingualism and Internationalised Domain Names (IDNs), IGF initiatives from Macedonia, Nepal, Russia, and South Eastern Europe spoke about the value of IDNs as promoters of diversity of languages and cultures online. Despite their potential to encourage more people to use the Internet, IDNs still face uptake challenges.

Digital currencies and blockchain technology were the focus of a session co-organised by IGFs from Armenia, Brazil, China, and Nigeria. A key message pointed to the significant potential of using blockchain across different systems (i.e., public institutions, the financial sector, etc.), to improve the security of data and the stability of systems. As for digital currencies, they could co-exist with traditional banking systems, if the risks of abuse by criminals are tackled adequately.

DON'T MISS TODAY

Dynamic coalitions: Contribute to the digital future!
10:00 – 11:30 | Main Hall (Room XVII - E)
Thirteen IGF Dynamic Coalitions will come together during this session to showcase their work on technical, rights-related, and other Internet issues: accessibility and disability, community connectivity, innovative approaches to connecting the unconnected, public access in libraries. The Internet of Things, blockchain technologies, network neutrality, platform responsibility, child safety online, gender and Internet governance, trade, publicness, core Internet values, and Internet rights and principles.

NRIs perspectives: Rights in the digital world
11:30 – 13:00 and 15:00 – 16:00 | Main Hall (Room XVII - E)
National, regional, and youth IGF initiatives will share their perspectives on rights in the digital world. They will ask how the development of new technologies is affecting our digital rights. What are the challenges and limitations in exercising such rights, and how can they be most effectively addressed? Can the multistakeholder model provide meaningful solutions to problems already identified?

Gender inclusion and the future of the Internet
16:00 – 18:00 | Main Hall (Room XVII - E)
What does it mean to integrate gender into Internet governance processes? How can this be done, what are the challenges, and how can they be addressed? These are some of the questions to be discussed during the session, which will also look at issues such as access and the gender digital divide (including in relation to new and emerging technologies) and online gender-based violence.