*IGF Daily* **No. 1** – Tuesday, 13th November, 2018

# IGF Daily

REPORTING DAILY FROM THE
13th INTERNET GOVERNANCE FORUM

dig.watch/igf2018

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

## CHANGE AT A HISTORICAL MOMENT

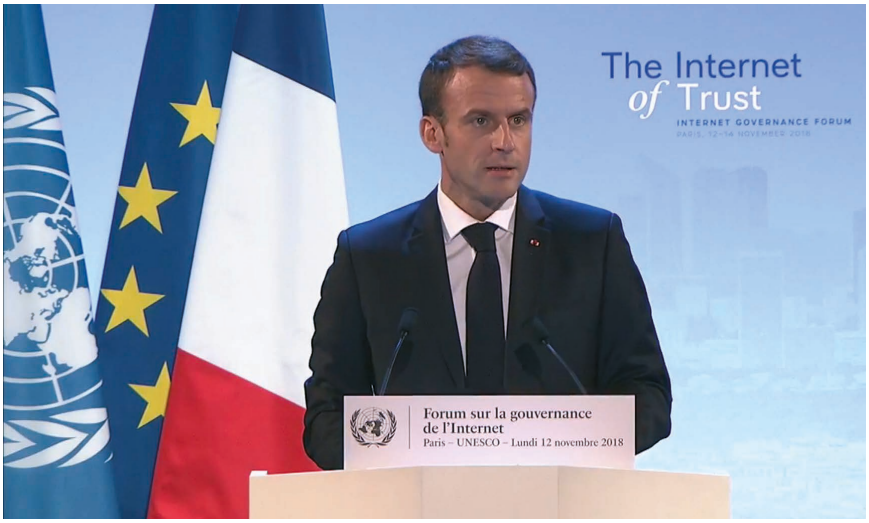
'In the lecture halls and cafes of Paris, philosophers and writers have been discussing the interplay between technology and humanity for centuries.' Our time is no different. Global debate on the interplay between technology and humans is needed more than ever before. This was the underlying message of the UN Secretary General's opening speech at the 13th Internet Governance Forum (IGF).

IGF 2018 is a turning point in digital policy. This was felt yesterday in the IGF conference rooms and corridors. In Paris, while celebrating 100 years since the Armistice, the digital community embarked on a discussion of the future of Internet Governance (IG). If the IGF wants its core mission to remain the same, the way it operates must evolve. The need for change and a new vision for the future echoed in the opening speeches of UN Secretary-General Antonio Guterres and President of France Emmanuel Macron. The two speeches were much more than diplomatic routines. They were substantive reflections on the present moment, and bold visions for the digital development ahead of us.

Concrete proposals were not missing from these speeches. UN Secretary-General Guterres clearly outlined parameters for the IGF 2.0. The IGF should be not only multistakeholder but also multidisciplinary. Philosophers and anthropologists, among others, will be needed more and more in debating questions of ethics and the future use of technology. The IGF should find innovative solutions to bridge the increasingly fortified policy silos of the technical, security, business, and other communities. New thinking, shared language, and reframing of existing narratives are needed to deal with digital challenges.

The UN Secretary-General invited the IGF community to listen to the unheard and marginalised voices from local communities, people with disabilities, youth, and the elderly. Digital growth affects us all, yet many remain outside of current debates.

President Macron sent an equally clear message for a strengthened IGF which should provide concrete policy outputs. The IGF needs more resources, a robust structure, and higher policy relevance in the UN system. He called on the IGF to monitor implementation of the Paris Call for Trust and Security in Cyberspace, a high-level declaration on developing common principles for securing cyberspace. The Paris Call builds on the WSIS Tunis Agenda's definition of the 'respective roles' of states and other stakeholders. It also resonates with the UN Group of Governmental Experts (GGE) reaffirmation that international law applies to cyberspace. The Paris Call has strong initial support from hundreds of signatories, including leading tech companies and many governments. Yet the USA, Russia, and China are missing. It remains to be seen if the Paris Call will create new convergences in global cyberpolitics. In this process, the IGF can play an important role.




French President Emmanuel Macron addressing the 13th IGF in Paris
*Credit: IGF Secretariat*

# IGF Daily

## HIGHLIGHTS FROM DAY 1

**With over 150 workshops, open forum sessions, high-level meetings, and other gatherings spread over three days, the range of digital policy topics discussed at the IGF is broad. The following thematic summaries cover Day 1, based on the *Digital Watch* taxonomy. Additional coverage will be provided in our final report.**

### Technology *and Infrastructure*

Emerging technologies fascinate us. They open new possibilities and create new challenges. Yet, 'technology does not solve humanity's problems' said Google's CEO Sundar Pichai in his recent interview for *The New York Times*. 'Technology is an enabler, but humanity has to deal with humanity's problem'. Day 1 discussions at the IGF echoed this sobering message from a tech leader.

Many of these discussions revolved around ethics and the need to ensure that technologies are 'pro-people'. Taking artificial intelligence (AI) as an example, one starting point is to bring more transparency into AI systems, so that non-specialists can understand how they work.

Documenting work processes in a transparent manner, and allowing for more oversight into mathematical formulas behind automated decisions can certainly help. AI can be biased and contextual, because AI algorithms are driven not only by code, but also by data. If we feed an algorithm with incomplete data, that can lead to bias and discrimination. Ensuring that we align emerging technologies with ethical and socio-economic considerations could help advance a more inclusive digital economy.

Emerging technologies like AI depend on high speed Internet. However, in some parts of the world, connectivity itself is the challenge. Improving access to the backbone of the Internet is vital for addressing the digital divide worldwide.

At the national level, one way of achieving greater connectivity is through community networks. There are many examples of successful community network projects, run or supported by organisations such as the Internet Society, AlterMundi and Guifi.net. But there are also difficulties in setting up such networks, from challenging regulatory frameworks to barriers in accessing and using spectrum resources.

### Cyber*security*

Dealing with global risks featured prominently in yesterday's discussions on cybersecurity. In wartime, international law provides a set of rules for state behaviour. But what about ensuring cybersecurity in times of peace?

The Global Commission on the Stability of Cyberspace (GCSC) reiterated its proposed set of voluntary norms for state and non-state behaviour, centered on the protection of the public core of the Internet. The public core includes the physical infrastructure of cable systems, the transmission of communications, cryptographic keys for authenticating users and devices and securing Internet transactions, and the Internet's address book of names and numbers. The norms say that states should respect the principles of due diligence, good governance, and neighbourliness in their behaviour to prevent attacks originating from their own territories, in particular by non-state actors.

Some states may not agree with these suggestions. Disagreements reflect deep political and conceptual differencies. How can countries be encouraged to endorse and adhere to norms? A helpful measure is to explore further the concept of (cyber)sovereignty.

When it comes to the private sector's behaviour, offensive measures to defend against cyber-attacks, known as hack-backs, can cause additional security consequences and are also illegal in some countries.

Discussions also turned to encryption: due to a shift to so-called service-centric networking – where most services are provided in the cloud rather than based on software installed on our devices – service providers need to integrate encryption more strongly into these services. This is particularly important for Internet of Things applications.

**Day 1's most prominent issues**

DiploFoundation's Data Team analysed the most salient issues across 39 transcripts captured from real-time captioning, which were then processed using a custom digital policy dictionary. The exercise was automated with the assistance of text analysis software that helped the team sort through retrieved content according to the *Digital Watch* taxonomy.

## HIGHLIGHTS FROM DAY 1

### Legal *& economic*

Legal and economic issues came into focus during Day 1's main session on emerging technologies and AI. In particular, participants raised the question of the potential harmful impact of AI on human society. For example, lethal autonomous weapons systems have attracted much concern from actors worldwide.

The discussion on the impact of AI and ethical considerations triggers reflections on the relationship between law and ethics. Ethics is usually at the basis of law; some ethical rules are in fact codified into law. However, ethics goes much beyond law in organising a wide range of family and community relations. Further, ethics is not a substitute for law. This complex interplay between law and ethics has implications for many issues related to AI technology.

The question of whether mathematical formulas are able to deal with law emerged from the discussions. Formulas are subjective: they are applied based on what the developer thinks is fair and appropriate. Unlike a human judge applying a legal rule, machines cannot contextualise issues.

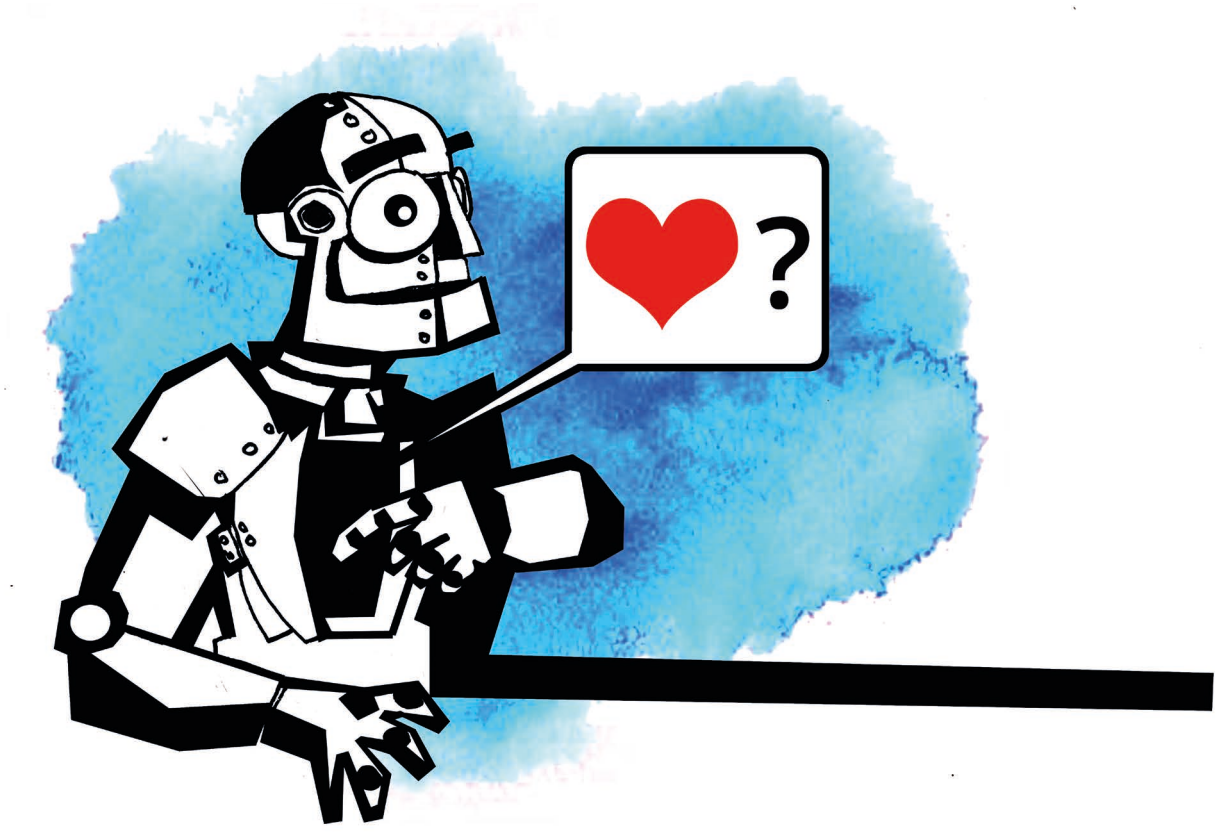
### Human *rights*

Threats to freedom of expression and privacy, and the persistent gender digital divide, dominated the discussions on human rights issues on Day 1.

Unfettered access to data is eroding users' privacy. This is one of the main findings of Freedom House's latest *Freedom on the Net* report. Online manipulation was another important threat identified in the report. The growing number of cases of blocking, filtering, and Internet shutdowns continues to threaten the Internet's freedom. In some cases, stakeholders shy away from discussion of these issues, and this makes it more difficult to have meaningful multistakeholder dialogues, conducive to solutions.

Focusing on the Middle East, one session discussed the need to design and develop predictable legislation and legal frameworks on privacy and data protection to support business activity. With several global models to follow, data protection is actually an enabler for businesses, due to the advantages it offers to companies with international activities.

The gender digital divide continues to persist in low income countries, due to cultural beliefs that tend to favour males over females. Women's access to technology is often restricted or monitored by their own family members. This hampers any possibility for women to be equally represented in the technology field or to participate on equal footing with men in politics.



## HIGHLIGHTS FROM DAY 1

### Development

Development discussions during Day 1 emphasised that digital tools are essential for achieving the SDGs. The open forum organised by the UN Secretary-General's High-level Panel on Digital Cooperation introduced digital public goods as a conceptual framework to address the digital divide. In many cases, governments, the private sector, and other actors have provided digital public goods, however there is not yet sufficient coordination and cooperation in such initiatives.

Narrowing the digital divide takes more than providing access to a the Internet. If people do not have adequate technical skills, knowledge, and an enabling regulatory framework, they cannot use digital technologies to their full potential.

Digital inclusion is particularly important for refugees, for whom access to information and the Internet is a basic need. For people on the move across borders worldwide, the Internet facilitate integration in the new country, and allows them to remain in touch with loved ones in the country of origin.

While many sessions confirmed the need for capacity development in Internet governance, one session focused on practical steps to achieve capacity development. How do we avoid competition, create meaningful cooperation and partnerships between various actors, and ensure sustainable impact? When looking at financing models, session participants highlighted core funding for capacity development providers as ideal in allowing the providers space to continuously adjust activities and learn from their experiences.

### Socio-*cultural*

The Day 1 discussions reaffirmed the old insight that technology can be used both for good, and for less beneficial purposes: it can be a medium for hate speech or promoting violence and terrorism. We are currently seeing an increase of extreme ideas in mainstream political discussions online, but a decline in the acceptance of the rights of others.

How can hate speech be countered or dealt with, and who has the responsibility to do so? Many stakeholders can be involved, to different extents. Content removal is a delicate issue that requires cooperation and carefully calibrated checks-and-balances among civil society, governments, and the private sector. However, dangerous content such as online hate speech needs to be understood in a broader context: removing content is an immediate solution that addresses only the symptoms of the problem; the causes go much deeper and require long-term education and the promotion of tolerant and inclusive public debates. Content policy is a major challenge for social media platforms. They have to recruit legions of content supervisors. Often these content specialists lack the understanding of local culture and the language skills that are essential for addresses problematic content, such as hate speech, appropriately.

'Information disorder' emerged as a potential alternative term for 'fake news'. This term might capture more accurately situations when published information is factually accurate, but is released with malicious intent and used by political adversaries to undermine the credibility of independent information providers.

Many actors have roles and obligations in dealing with information disorder. Participants in some sessions asked whether digital intermediaries (for instance, social media networks) were the *de facto* gatekeepers of content. Others warned against the concentration of regulatory power in the hands of just one actor, be it the private sector or government.


### PARIS DIGITAL WEEK

All eyes are set on Paris this week. The City of Lights is hosting three high-level political events: the 13th Internet Governance Forum, hosted at UNESCO's headquarters; the Paris Peace Forum; and the GovTech Summit. The Paris Peace Forum began on the Centenary of Armistice Day and has brought together 'all actors of global governance' who are determined to uphold multilateral cooperation and tackle pressing global challenges. The GovTech Summit gathered world leaders, investors, and innovators who discussed how new technologies can help deliver better public services to citizens and promote democracy.