Government Offices of Sweden

31 January 2019
UD2019/

Ministry for Foreign Affairs
Department for International Law, Human Rights
and Treaty Law

Sweden's contribution to the UN High-Level Panel on Digital Cooperation

1. VALUES AND PRINCIPLES

Human rights, democracy and the rule of law (1a)

The key values that should underpin cooperation in the digital realm are **human rights**, democracy and the rule of law. This includes for example the Universal Declaration of Human Rights as well as the International Covenants on Civil and Political Rights and Economic, Social and Cultural Rights. International law is essential and applicable in the digital realm.

Human rights apply online as well as offline, and we must ensure that they are respected, promoted and protected also in international cooperation on digital issues. The same human rights, responsibilities and obligations granted upon individuals and states of the physical world must also apply in the digital world. Although human rights are universal and indivisible, some are particularly central to the internet, including (but not limited to) freedom of expression and opinion, freedom of association and assembly, privacy and freedom of information.

The internet and other digital technologies have great potential to promote and enhance the enjoyment of human rights, democracy as well as sustainable development. ICT is an important tool for democracy as it enables more people to participate in democratic processes and dialogue. However, we must also recognise the challenges that exist, including the way in which human rights are sometimes restricted, and the global trend of shrinking democratic space which also manifests itself online.

Telephone: +46 8 405 10 00
Fax: +46 8 723 11 76
Web: www.regeringen.se

Postal address: SE 103 39 Stockholm
Visitors' address: Tegelbacken 2
Email: foreign.registrator@gov.se

Human rights, democracy and the rule of law must be respected and secured by states, and form the base for all standards and regulations for cyberspace, including in the areas of cybersecurity and counter-terrorism.

An open, free, secure, accessible and inclusive internet (1a)

It is crucial that the internet remains **open, free and secure with equal access and inclusiveness for all**, in compliance with international law.

The potential for Information and Communication Technologies (ICTs) is significant in theory, but many barriers remain when it comes to access and effective use of these tools. Around 50% of the world population is still offline. Governments and the private sector must address these barriers through innovative technology and new business models to stimulate affordability and improve connectivity. Increased meaningful access must remain a priority as we have seen how the growth rate of new internet users has declined in recent years.

Addressing the gender digital divide is of the outmost importance, especially as the divide is widening. Unequal access to digital tools and internet threatens to exacerbate existing inequalities.

The global trend of shrinking democratic space is affecting women's opportunities to access, participate and contribute through ICTs, and is thereby reinforcing the digital divide. At the same time, it may be noted that the online space in many contexts of shrinking space often is one of few public spaces accessible to women.

Using the potentials of the internet and adopting a human rights-based approach to the challenges (1a/b/3a)

While there are obvious challenges to the internet and digital technologies, these must be viewed as a negative side-effect of otherwise extraordinary positive developments. Thanks to the internet and social media, human rights are more widely known worldwide than ever before, and ICT has played a positive role in our everyday lives, our democracy and our economy. It is up to us to tackle the threats and promote the potential. And it is vital that these threats are solved without human rights being limited.

It is important to bear in mind that vibrant and pluralistic discussions are preconditions for a democratic, inclusive and diverse society. The internet's capacity to bring people and politicians closer to one another must not be weakened. By limiting the enjoyment of human rights on the internet, we are limiting development.

That is why we argue that a human rights-based approach in all discussions concerning the opportunities and challenges opened up by digitalisation, including cyber security, is essential if more persons are to be able to have access to a free, open and safe internet.

A human rights-based approach means, among other things, that internet-related laws, policies, practices and decision-making processes should protect and respect international law, including human rights. They should not be used as a pretext to violate, abuse or limit human rights. They should be developed through open, inclusive and transparent approaches that involve all stakeholders. In addition, education, training and digital literacy should be promoted to realise human rights online.

A multi-stakeholder model for cooperation (1a/3c)

We underline the importance of participating alongside other stakeholders in a **multi-stakeholder system** in developing the framework, content and common standards of the internet. This should include a range of different stakeholders from government to industry to civil society, including human rights defenders. This multi-stakeholder model is absolute key, and governments need to acknowledge the expertise within civil society organisations and the role of the private sector and technological community. Increased influence by governments at the expense of other stakeholders cannot be accepted.

A multi-stakeholder system should be open and accessible to all stakeholders, whose views should be heard and considered. It should be transparent and enable a broad dialogue and meaningful participation for all stakeholders. The internet is global and must be addressed with this in mind.

The internet and digital issues are discussed in various fora and from many angles, and we need to consider the added value of any additional fora or mechanisms to deal with these issues. Furthermore, we are not convinced that any new international legal frameworks should be created. For example,

the scope of the ITU should not be broadened to internet related issues that are dealt with in other multilateral fora (e.g. UNESCO, CTED, IGF etc.).

From a cyber security policy perspective (1a)

The digital domain exists within a rules-based international order, based on norms and principles, agreed by the international community. The core is international law, including human rights and fundamental freedoms.

Digital connectivity promotes peace, security and global development, as repeatedly stated in international agreements and fora, including within and by the UN. The core is **a global, free, open, accessible, secure and stable cyberspace**.

A global, free, open, accessible, secure and stable cyberspace is ultimately based on trust between states, companies, institutions and individuals alike. The core is therefore to achieve mutual trust between all stakeholders.

2. METHODS AND MECHANISMS

Access and digital divides (2a/b/c)

Our development cooperation is guided by a human rights-based approach, and we support the ecosystem of a free open and secure internet as a key enabler of sustainable development. Support includes multi-stakeholder tools, such as the development of the UNESCO Internet Universality Indicators. We also support participation of civil society in internet governance as well as in normative and legislative processes on global, regional and national level.

Cost remains one of the greatest barriers to network and internet access and with declining growth of new users we should find ways to support new business models and innovative ways of connecting the remaining half of humanity.

Many forms of digital divides remain between and within countries, and between women and men, boys and girls – a gap which should be closed. This includes addressing disparities in access to and use of ICT, which

undermines women's full enjoyment of their human rights. This issue has been recognised in the Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the Internet, as well as in the OHCHR report on gender digital divides which provides an excellent starting point in the work to bridge it.

On a national level, platforms for multi-stakeholder dialogue, that includes government, service providers, civil society and academia, should focus on better understanding the digital divides and finding common solutions to bridging them.

From a cyber security policy perspective (2a/c)

Methods and mechanisms that we promote when it comes to cyber security cooperation:

- Global and regional dialogue and cooperation between states to agree on and implement norms for responsible state behaviour, based on international law and international agreements.

- Multi-stakeholder dialogue and cooperation on global, regional and national levels to manage, develop and maintain digital flows of information and digital governance/governance of the internet.

- Confidence building measures on national, regional and global levels, which includes information sharing, dialogue, and practical cooperation on technical and operative levels.

- Capacity building, both to support digitalisation and to strengthen cyber security and resilience, on national level as well as through international cooperation and sharing of expertise.

- Mainstreaming of the ICT, cyber, digital challenges into foreign and security policies and processes on a national level as well as within bi- and multilateral cooperation. Development of cyber diplomatic tools and dialogue.

- Cooperation and dialogue between the public and private sector on national and international levels.

3. ILLUSTRATIVE ACTION AREAS

Challenges (3a)

Respect for human rights on the internet needs to be strengthened worldwide, and the challenges of online safety is used by many to justify far-reaching violations and abuses of human rights with the argument that a balance must be struck between rights and security. States are building up capacity for exercising surveillance and persecuting human rights defenders, journalists and other media actors, political opponents and others exercising their rights online. This trend can and must be seen in the context of the **global trend of a shrinking democratic space**.

There is an increasing amount of repressive legislation and regulation, administrative measures and harassment online and offline, which covers everything from restricting access, blocking sites and shutdowns of services, to rules limiting financing opportunities for individuals, companies and organisations. This not only limits freedom of opinion and expression, as well as of freedom of assembly and association, but also individuals' opportunities to actively participate in and contribute to the societies where they live. It also limits their chances to influence decision-making and, ultimately, how countries are governed and undermining the very foundation of **democracy**.

As cyber security threats are increasing in frequency and sophistication, asking for more innovative solutions, this creates a growing need for all stakeholders to work together to address these issues **in a manner that promotes and respects human rights**. The argument of security versus human rights is not a valid one. We believe that human rights and security are complementary, mutually reinforcing and interdependent, and that they are both essential for the promotion of freedom and security. Cyber security should always be addressed through a **human rights-based approach** (see above 1a), with the individual at the core. States must respect their international human rights obligations, including when implementing laws nationally.

To continue working to promote human rights, on the internet and elsewhere, is also crucial to counter growing **propaganda and**

disinformation activity from states and from terrorists and extremist groups or other actors striving to undermine human rights, democracy and the rule of law. Supporting independent journalism and a pluralistic media environment as well as protecting the safety of journalists and other media actors is central in this context. Stronger initiatives to improve media and information literacy, especially among young persons, and promoting greater knowledge of and access to technology, media and information in general are also important components in this work.

Successful examples, and forms of cooperation (3b/2c):

We would like to underline the importance of making the best use of, developing and protecting existing mechanisms, tools and instruments rather than aiming to create new ones. When it comes to the legal framework, international law, including human rights, applies online as well as offline and we do not see the need for any new international legal frameworks.

Good examples of cooperation, mechanisms and tools (3b/2c):

- Four UN HRC resolution on "The promotion, protection and enjoyment of human rights on the Internet", all adopted by consensus in 2012, 2014, 2016 and 2018
- UNESCO ROAM principles and Internet Universality Indicators
- Freedom Online Coalition (e.g. statement and recommendations on a human rights-based approach to cyber security)
- UN Guiding Principles for Business and Human Rights (private sector)
- Global Network Initiative (private sector)
- OHCHR report on Gender Digital Divides
- Internet Governance Forum as a multi-stakeholder platform
- Stockholm Internet Forum – development focus, interactive meeting with a multi-stakeholder approach

- Council of Europe and OSCE work on the internet and human rights, democracy and the rule of law

- WSIS outcome documents.

From a cyber security policy perspective (3b/c/2c):

- Implementation of GGE 2013, 2015 reports and coming UN process (GGE, OEWG, IGF)

- Voluntary international dialogues and initiatives to forward norms outside the context of the UN (eg. GCSC, Paris Call, Freedom online Coalition etc), including through multi-stakeholder dialogue

- International cooperation on capacity building, within and outside the UN (eg. GFCE)

- Cyber-diplomatic dialogues (eg. EU with China, India, US etc; Nordic and Nordic-Baltic cyber dialogues)

- Regional cooperation; implementation of OSCE Confidence Building Measures (CBM:s)

- Regional cooperation; digital internal market and cyber security cooperation within the EU

- Development of EU cyber diplomacy toolbox to handle malicious activities in cyberspace (including joint statements and sanctions).

- Adoption of national strategies for digitalisation as well as cyber security