EUROPEAN PARLIAMENT 2009 - 2014

Committee on Foreign Affairs

13.6.2012

WORKING DOCUMENT

on a digital freedom strategy in EU foreign policy
Committee on Foreign Affairs

Rapporteur: Marietje Schaake

"By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole." - Frank La Rue[1]

Digital Freedom in the EU's External Actions

Internet and new technologies play an exponentially important role in the lives of Europeans, and in fact, of citizens everywhere. We stay connected with friends and family online, we read or watch the news on our smart phones, we have instant access to an ever expanding database of information, companies trade and invest on digital market places, public procurement is processed more easily, music and video on demand have become an integral part of the way we access culture, and election campaigns are hard to imagine without Twitter, Facebook and YouTube.

Several EU Member States have identified access to internet as a fundamental right, and the European Commission agrees digital freedoms are part of the Copenhagen criteria. Last year the European Commission launched the "No Disconnect Strategy" and digital freedoms are an increasingly important element of projects through the European Instrument for Human Rights and Democracy.

Not only in Europe, but globally technologies are changing societies, the functioning of our democracies, economies, businesses, media, development strategies, security and defence concerns and human rights issues. Information and power monopolies that have been unchallenged for a long time are upset.

Egyptians assembled on social media around the violent death of one man, a movement that kicked off the ousting of a thirty year long dictatorship. We are eye witness to the human rights violations in Syria through the roughly 100.000 clips that have been uploaded on YouTube.

Defence ministries across the world, as well as NATO, are struggling to assess new technological threats to our lives and societies and to find appropriate answers to them.

Farmers in Kenya know to which market to walk a 4 hour-long journey with their crops, as a text message informs them where demand will be.

In a globally connected world the EU should have a strategy to deal with new technologies in its external actions. There are several areas in this digital world in which it is essential that the EU acts as a global player and leverages its economic and political weight. Though overregulation would rather hurt than help the potential of the open internet, in some areas rules may need to be updated to match the revolutionary impact of technological developments with adequate democratic oversight.

This discussion paper seeks to invite suggestions on what the first EU's Digital Freedom Strategy in its External Actions might look like. The paper will be shared with Members of European Parliament and will be placed online to invite various stakeholders to provide input through crowd-sourcing.

[1] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, May 2011 - http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Security and freedom

New technologies challenge the way in which governments perform their core tasks. Defence and security ultimately lie in the hands of government; however, these increasingly rely on private players. This requires new forms of cooperation and shared responsibilities. There is no public sphere online, and this leads to changing chains of command. Only recently the European Parliament considered ICT infrastructure as critical infrastructure. Meanwhile debates about cyber warfare rage. Governments need to act responsibly by adhering to basic international public and humanitarian law principles, by respecting national sovereignty and human rights when using new technologies in giving substance to their duties. Given the EU's common security and defence policy as well as its economic interests, we should lead globally in balancing security and freedom. Some EU Member States, such as Estonia, have learned from experience after having been subject to cyber attacks.

In the past month the new Flame virus replaced Stuxnet in the list of modern day attacks. Leaks from the White House suggest these tools are US made and used to target Iran's nuclear program. In the broader context, questions of attribution (who can be held accountable for an attack), whether a cyber attack can constitute an act of war, and the relevance of invoking NATO's article 5 (an attack on one is an attack on all) are vividly debated.

Cyber warfare as well as perceived threats can easily spin out of control and lead to major unintended consequences. Aside from EU citizens also third country nationals are affected by protective measures, as came to light when internet users in Iran where in danger after the database of a Dutch issuing authority of encrypted information protocols was hacked and used to monitor internet traffic.

Human rights

A quick scan of some events in the world shows that the struggle for human rights has moved online. Prisons are increasingly populated by dissidents confronted with their own internet and mobile communications, compromised by the authorities.

Iran continues building an electronic curtain, which eventually will cut off the Iranians from the World Wide Web through the creation of a 'Halal internet'. Iranians challenge and circumvent this mass censorship in innovative technological ways, finding their way to stay connected. Human rights defenders deserve EU support and in any case should not be targeted with tools and technologies developed and exported from within the EU.

China is similarly cutting its citizens off of the open internet with the great electronic firewall. Mass censorship violates citizen rights and narrows business opportunities. Plans are on the table to make anonymous blogging in China illegal.

The Ben Ali government of Tunisia, as well as the Al Assad regime in Syria are well known for their sophisticated use of technologies against citizens. The Syrian Electronic Army is now subject to ad hoc EU sanctions.

Generally speaking, the fight for control and power by authoritarian regimes involves a growing ICT component. Promoting and defending human rights then means enabling people to circumvent mass censorship or to evade cyber attacks by their own governments. While training *netizens* should improve their safety online it also creates a new set of sensitivities

and a potentially dangerous dependency on the accuracy and quality of the guidance. This responsibility should not be underestimated and has to be reflected in the ways and means we use to assist citizens, bloggers, citizens journalists and human rights defenders online.

Trade and export

Besides ad hoc export restrictions and trade sanctions, the digital and globally connected reality calls for awareness and responsibility in European corporate boardrooms. It also requires comprehensive and permanent export restrictions to limit the harmful potential of sophisticated, targeted technology systems. Technologies, tools or services custom made for targeted human rights violations should not be allowed on European markets at all. These systems should be categorized as 'single use' technologies and do not differ from traditionally banned torture tools or (parts of) weapons of mass destruction in their impact.

While the recent EU export bans on certain elements of technologies to Syria and Iran are an important first step, they risk becoming a paper reality, threatening the EU's credibility, and the safety of citizens who think they can rely on the EU's efforts and promises. Instead of leaving enforcement up to the different member states, the European Commission should have the powers and tools to monitor the proper implementation of these restrictions. Transparency and accountability are needed in this field, much the same as we verify the quality of foods and medicine, or conventional weapons. This requires innovative policies such as non-financial disclosure requirements and updated reporting standards.

Additionally, the European Commission should be able to provide companies, in doubt whether to file for an export license, with real time information about the legality or potential harmful effects of trade deals. The same goes for EU (based) companies that enter into contractual relations with third country governments, whether to win operating licenses, negotiate standstill clauses or by accepting public involvement in business operations or public use of their networks and services.

Business interests

EU policies need to be smart and custom made not to restrict the export of potentially 'liberating' technologies. This is not merely a human rights issue but also directly impacts the business opportunities of EU based companies. The involvement of Vodafone when the Mubarak government successfully used the internet 'kill switch' while sending government propaganda to its Egyptian users has been widely discussed and scrutinized. The transition government in Egypt has since tried the responsible ministers, focusing on the economic losses but leaving the societal and human rights impact out of the picture.

While Vodafone's conduct has been criticized, and should be formally investigated, the case raises the question whether the EU should not back its businesses with more political support in these circumstances. One way is to make the conclusion of new free trade agreements conditional on the preservation of the open internet, or to provide ad hoc political backing. Would Vodafone have acted differently if the EU's Commissioner for International Trade or the High Representative for Foreign Affairs would have interfered and supported the company in rejecting the order to terminate all mobile and internet traffic?

The responses by both Yahoo and Google to the Chinese government's policies of censorship

and demands of oversight and control over business operations indicate that the changing balance of global powers also affect businesses and require joint efforts with European policymakers and civil society actors.

Internet governance

The internet is governed by a so-called multi-stakeholder approach, which has been developed organically into a network of public and private actors. In 2005 it was decided that the Internet Governance Forum would be the main international platform for discussion, which is convened by the United Nations.

The multi-stakeholder approach ensures that all stakeholders have a seat at the table. This inclusive approach has ensured the openness of the internet, which is the catalyst for many societal benefits.

There are currently two threats to this system of governance. Developed countries are drafting legislation behind closed doors where only few corporate stakeholders have a say in the proceedings. Meanwhile the impact of proposed laws touches the very infrastructure of the internet. In the meantime and largely below the radar, coalitions of emerging economies are joining forces to introduce a global regulatory framework for the internet, including increased state control and establishing an UN regulatory body. A new era of global internet politics has kicked off.

While the EU is the world's most significant market, most internet companies are US based, which forces European citizens to accept US user conditions. As most online services are US-based internet users world-wide often fall within US jurisdiction when using these services. This extraterritorial impact of US laws should not restrain the EU's ability to defend the fundamental rights of citizens.

It is key for policymakers to understand that in a globally connected world parameters of lawmaking are constantly changing and traditional concepts of set jurisdictions often do not match our global digital hemisphere. This however does not preclude the possibility of efficient dispute settlement mechanisms or addressing conflicting jurisdiction.

Credibility

The EU can not credibly promote and protect digital freedoms in the world if they are not safeguarded at home. Although restrictions to freedom online sometimes are lawful there is an overarching impact on our credibility and moral standing in the world. The UK was commended by Chinese and Iranian authorities and offered assistance in blocking instant messaging services during the London riots in August 2011.

More pressingly, the same tools and technologies that our governments and law enforcement agencies can use to (lawfully) intercept mobile or internet traffic can have a fundamentally different impact on citizens in societies where the rule of law is absent or no separation of powers exists. The context in which technologies are used is of essential relevance. Can we speak of ´lawful interception´ technologies in a society without the rule of law? The use and development of these tools and technological capabilities do not exist in a vacuum but are inextricably linked to the context they are used in. Technologies create wonderful opportunities and can contribute to our freedoms, but in the hands of dictators the same

technologies can become effective weapons.

The European Commission is currently developing a set of human rights (and also broader corporate social responsibility) guidelines for the ICT sector, based on the UN Guiding Principles for Business & Human Rights (Ruggie principles). Whilst these guidelines will not legally bind European companies they might prove to be a useful framework for ICT companies in mainstreaming human rights concerns and in performing impact assessments, even at the R&D phase or when filing for patents. These guidelines will also contribute to a level playing field in the EU's internal market.

Development

The EU should make its development policies more efficient and effective through embracing ICT. The EU can help bridge the digital divide; either by building and installing basic ICT infrastructures, by providing access to knowledge, information and payment services to let local economies bloom, or by using ICT to share information about health issues. The EU could enable (online) education in remote areas by developing and providing cheap wirelessly connected tablets, allowing parents to let their children go to school.

In the first critical hours after natural disasters or during humanitarian crisis ad hoc emergency telephone and internet connections should be set up. ICT solutions should be amongst the most basic tools and instruments in all of the EU's development programs, including in the work and programmes of the EU Delegations all over the world.

Development programmes should also include the protection of digital freedoms in a structural way, in particular by planting seeds in early post-conflict or political transitions. EU regulators or regulatory experts should engage with their counterparts. Embedding basic rights principles in new (media) legislation is an essential safeguard and should prevent the inclusion of provision in laws that for instance make encryption illegal, like in Egypt is currently the case. These laws can have unintended effects that a newly or (first time) elected parliaments or governments are not necessarily aware of.

Finally, by connecting millions of people in developing countries, or by keeping them online, to the internet, social media and letting them tap into the online cloud not only development flourishes, but also innovation can benefit from increased collaborative efforts.

Digital Diplomacy

The internet and particularly social media enable governments to engage in direct diplomacy and allows increased people-to-people contact around the world. Open debates about ideas can refute extremism and improve intercultural engagement and understanding.

The EU should also make its diverse cultural content more accessible to people around the world via increased investment in digital and cultural diplomacy. The EU is among the richest and most culturally diverse areas in the world, but is doing too little to take a leadership position opening up culture and knowledge to people across the world.

By allowing more people to connect without being censored, more people can access information and cultural content. Culture can facilitate access and contact where political relations are blocked or troubled. Culture, values and freedoms are very much intertwined; it's therefore also a strategic issue for Europe.

The opportunities for global connectivity around European cultural content should be celebrated and facilitated, for example, through Europeana, or websites of museums and festivals.

The economic potential of the EU as a global digital player is best served by a reform of Intellectual Property Rights laws and the completion of the European digital market. Only then we can ensure that the wealth of our (digitized) cultural diversity is accessible and marketable across the globe.

And last but not least, the European Institutions can contribute a great deal to making the European political culture and decision making process more accessible to citizens across the world. Through open data, transparency and access to information are further developed.

The European Parliament should commit itself to including new technologies in the work of its delegations with other parliaments across the globe, and will keep a close watch on the progress and concrete measures taken to devise an EU strategy on digital freedom in its external relations. A proposed assessment in annual reports should ensure accountability and continuity.

Digital Freedom Strategy

Our digital freedoms, including the uncensored access to information and communication, are universal rights and are indispensable for traditional human rights such as freedom of expression and freedom of assembly, and also for ensuring transparency and accountability in public life. Human rights violations are documented and shared with the help of mobile phones. The EU should take the lead in globally promoting and protecting digital freedoms. Besides being the world's largest trade block the EU is also a community of values, which should also be the core of all our external actions.

Only by synergising our trade, security and foreign policies, by aligning our values and interests the EU can fully leverage its power and act as a global player. As technology is developing so rapidly it is essential to promote structural collaboration between politicians, business and civil society. This ongoing equilibrium may best serve the open global internet, to everyone's benefit.

- Different branches of governments need to get aligned behind digital freedom
- Mainstreaming of digital freedoms in existing human rights and democracy projects
- Permanent ban on exports of intrusive or 'single use' technologies designed for violating human rights
- Increased transparency and accountability for businesses
- Ongoing dialogue and knowledge sharing between policymakers, businesses and No's
- Guidance and political backing of ICT companies by EU governments in third countries
- EU needs to strategize and take a multi-stakeholder approach in internet governance fora
- Only by respecting digital freedoms at home the EU can credibly defend them in the world
- Engage in direct or people-to-people digital diplomacy to exchange ideas and culture

- Support, train and empower *netizens* and human rights defenders to circumvent censorship and evade cyber attacks