SECURITY AND HUMAN RIGHTS MONITOR

Digital Freedom and Security in a Globally Connected World

Lessons from the MENA region

Marietje Schaake
Marietje Schaake is a Member of the European Parliament for the Dutch Democratic Party (D66) with the Alliance of Liberals and Democrats for Europe (ALDE) political group.

DOI: 10.1163/18750230-99900026

The Internet and new technologies play an exponentially important role in the lives of Europeans and citizens everywhere. Globally over 2,5 billion people have access to the internet. Online, we are connected with friends and family, where we also find expanding access to sources of information and wherebusinesses trade and invest on digital markets. Music and video on demand havebecome an integral part of the way people access culture and election campaignsare hard to imagine without social media.

These developments are also reflected in politics and impact democratic development. This revolutionary impact of technology has become particularly clear in the context of the uprisings in North Africa and the Middle East (MENA) that have taken place over the past couple of years. The empowerment ofindividuals through technologies disrupts existing monopolies of power andinformation. Online popular movements force governments to be moreaccountable, or to perform their basic public duties differently in a globally connected world where traditional borders fade along with the traditional parameters of lawmaking and jurisdiction. As a result, tasks traditionally in the hands of governments are now increasingly performed by private companies.

The realization of human rights such as freedom of expression, access to information and freedom of assembly increasingly depend on people's connectivity. If we want to continue to enjoy the many benefits and opportunitiestechnologies can offer, then security and trust, as well as digital freedoms are indispensable. They cannot become a zero-sum game.

The EU, as a global player, the largest trading-block and a community of values, should have a strategy to deal with new technologies as part of its foreignand security policies. And while over-regulation would hurt and not help the potential of the open internet, in some areas rules and laws deadling with principles such as human rights or competition need updating to adequately match the impact of technological developments and simultaneously establish adequate democratic oversight.

In December 2010, Egyptians assembled on social media around the killing of anordinary man at the hands of the police. The movement that developed kicked offthe ousting of Hosni Mubarak after thirty years of dictatorship. The Tunisian government of Ben Ali was infamous for its sophisticated use of technology to crack down on dissidents, and to censor information.

Today, we are eyewitnesses to grave human rights violations in Syria through hundreds of thousands of videoclips that have been uploaded on YouTube. The fact that a massacre, the killing of tens of thousands in the Syrian city of Hama in 1982, could remain unnoticed by the rest of the world for over two weeks would be impossible in current times. In today's hyperconnected world the inhabitants of Homs used the program Bambuser to broadcast live images of the shelling of residential neighbourhoods. The recent Internet blackout immediately raised international concerns over covert mass attacks by the regime against the population.

As we move from a scarcity to an abundance of information, wars are beingfought on the streets and we see 'information wars' online. Information and misinformation are spun and framed as uploaded online reports are difficult to verify in the absence of journalists on the ground.

Moreover, new forms of 'warfare' involving technology are increasingly institutionalized. Assad's 'Electronic Army' launches cyber attacks, tries to link opposition websites to terrorist organizations and tracks and traces bloggers. Both in terms of security and human rights, the lines between online and offline are blurring. This

underlines the need to improve the security and freedom of people online.

Reclaiming online territory

Governments across the world are seeking to regain control over people using technologies in an attempt to reclaim grip and control over increasingly empowered individuals. The consequences of these crackdowns are found in prisons that are populated by dissidents confronted with their own internet and mobile communications, compromised by the authorities. The Iranian government continues to build a 'Halal internet', which operates like a carefully censored intranet, which cuts off Iranians from the worldwide web. Iranian people in return courageously circumvent this mass censorship and surveillance in innovative technological ways to stay connected to communicate freely, to access information and to save lives.

It is not only in the MENA region that we find the deployment of technologies to repress and control people. In China people are cut off from the open internet through the blocking and filtering of content on a massive scale. A search for a term such as 'Tiananmen Square' may render no results in a search engine, and micro blogging sites are monitored and censored systematically. In Russia new laws legalize deep packed inspections into email and internet traffic.

Recently Ethiopia introduced draft legislation banning the use of VoiceoverInternet Protocol Services which are used for online chatting and calling. In Egypt activists found records of their conversations on Skype when they took over a (secret) police station, even though these voiceover IP technologies had been considered more difficult to eaves drop.

Clearly, denying unrestricted access to information and communication technologies violates citizen's rights but also narrows business opportunities. Moreover, aggressive technological systems do not only form a threat to people in repressive societies; they are also becoming an integral part of strategicsecurity questions.

Adjusting EU laws

The EU's stated goal of promoting and defending human rights will need to take shape differently and has to be updated to match the digital reality. Enabling people and grass-roots movements to circumvent mass censorship or to evade cyber attacks can be a part of human rights policies in this new context. While training human rights defenders should improve their safety online, it also createsa new set of sensitivities and a potentially dangerous dependency on the accuracyand quality of the guidance. This responsibility should not be underestimated andhas to be reflected in the ways and means we use to assist citizens, journalists and human rights defenders online. Knowledge of the implications of the use of technologies in various contexts is essential for the drafting of relevant foreign (as well as domestic) EU policies.

Some such policies are already developing in an ad hoc way. The EU has subjected Syria's electronic army to sanctions. We have also banned the export ofintrusive technologies that are used to monitor internet and mobile traffic with the single purpose of violating human rights. Operating monitoring centres,updating technologies or dispatching expert teams, such as Italian company AreaSpa did in Damascus, are now subject to sanctions. Similar restrictions have beenadopted towards Iran. There is, however, still a lack of an overall policy, which explains why exports to countries such as Bahrain continue despite the crackdown on citizens and human rights defenders.

In the process of mainstreaming policy approaches, it is important to distinguish between technology systems

that are designed to repress humanrights, and to identify these as ´single use´ technologies. This category should include ´the worst of the worst´ systems, and should include technologies that pose a serious security threat when in the hands of our adversaries. These need tobe distinguished from ´dual use´ technologies, which can be used for both 'good'and 'bad' purposes. The current digital arms trade from Europe to repressive regimes has to end.

We can not simply look at technologies in a stand alone manner. The context in which they are used needs closer scrutiny. The absence of the rule of law in a country should be considered before technologies that allow for ´lawful interception´ according to EU standards are exported.

Instead of creating a modern-day witch hunt of companies, we must seek the best way for companies and governments to be incentivized to do the right thing. Also, governments need to be aware of the challenges and pressurescompanies face when operating in countries with repressive regimes. This kindof collaboration should lead to a win-win situation for both human rights and business. We should ask ourselves for example, whether Vodafone would also have participated in shutting down the internet in Egypt or in sending propaganda text messages from the Mubarak government to its customers if the EU High Representative Catherine Ashton would have fully backed the companyin adhering to its European business standards and resisting such orders. Vodafone is after all the largest EU-based telecom company, and held the majority of shares of Vodafone Egypt. There is a lot to be learned about goodand worst practices when we look at the way in which ICT and telecom companies operated in countries in the MENA region, especially during the uprisings.

The EU needs to closely cooperate with businesses in order to be credible and effective. For that, the transparency and accountability of technology and telecom companies needs to be upgraded.

Additionally, the EU should more broadly use its economic leverage to ensure and enforce the promotion of human rights and the rule of law through itstrade agreements. Words and clauses need to be backed up by actions in order toretain our credibility. It will require the mainstreaming of the role of technologiesthroughout these external policies. To be successful and effective on the global stage the EU needs to invest in knowledge concerning technology so that it can become an integral part of foreign policy and its external actions.

Credibility in protecting human rights

In a globally connected world, it is increasingly difficult to separate domestic andforeign policies. Can the EU, the OSCE and other international organizations credibly promote and protect digital freedoms in the world if they are notsafeguarded at home? Although restrictions on freedom online are sometimes formally lawful, they can have an impact on our credibility and moral standing inthe world. A recent study by the Office of the Representative on Freedom of the Media on internet-related laws and regulations spanning the OSCE region showedthat much needs to be done to ensure that the internet remains an open and public forum for the freedom of opinion and expression. These important rights and principles are guaranteed by OSCE commitments and enshrined in the Universal Declaration of Human Rights and Permanent Council Decision No. 633 of 2004,which explicitly include the internet. The OSCE as well as the EU would improvetheir effectiveness by more strongly holding member states to the commitments they have made with regard to these freedoms.

The borderless environment online can lead to spill-over effects of our own actions in the EU that are not

always foreseen. Technologically speaking, tools tofilter spam can also be used to filter unwanted content for political reasons. And when the UK authorities proposed to block instant messaging when youngsters used this technology to communicate during riots, Iran and China were only too quick to show their understanding and to offer help in 'managing crowds'. Our political decisions at home have an effect on our credibility in the world, now more than ever. Also, technology is hard to contain. Once a tool of the system is available in one place, it will spread globally.

The same tools and technologies that our governments and law enforcement agencies 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 actually 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 areinextricably linked to the context in which they are used. Human rights impact assessments starting in the research and development phase can help assess the broader implications of further developing technologies. It is time to start working on the basis of human rights by design to make sure we put our most fundamental principles, and the well being of people first.

The threat to human rights can also come from vulnerabilities that remain unreported. Negligence impacting security online came to light when internet users in Iran where in danger after the database of a Dutch issuing authority of certificates was sabotaged and used to monitor internet traffic. Perhaps even more worrying, the Dutch government was aware of the security breach for 6 months but refrained from taking action or alert internet users.

All in all we are only seeing the tip of the iceberg of how technology impacts fundamental rights and democratic developments. On a regular basis, investigative journalists as well as individual experts discover new ways inwhich Western-based companies played a role in supplying the systems torepress people. The recent developments in the MENA region provide ample case studies. After the uprisings, the way in which technology can be used freely, or rather is used to repress will be a key indicator of the extent to which transitions towards more free, just and democratic societies are successful. Additionally, these cases reveal how much there is to improve for the EU to be a credible globalplayer.

Security in a connected world

New technologies also challenge and change the way in which European governments perform their core tasks. The responsibility for defence and securityultimately lies in the hands of governments; however, they increasingly rely on private actors. This requires new forms of cooperation, shared responsibilities and shifting chains of command. There is no space online that is owned by the public instead of companies, while the internet serves as a platform with increasing public value. The same is true for mobile networks. Only recently the European Parliament considered ICT infrastructure as critical infrastructure. Meanwhile debates about appropriate responses to cyber security concerns, cyberdefence and cyber warfare rage.

In the past month the Flame virus replaced Stuxnet in the list of modern- day attacks using technology. 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 attackon one is an attack on all) are being vividly debated. Cyber warfare as well as perceived threats can easily spin out of control and lead

to major unintended consequences. It is important to have objective threat assessments, instead of having to rely on cyber security companies and their studies. Given the EU's common security and defence policy as well as economic interests, we should lead globally in integrating security and freedom in the best possible way.

Synergy between freedom and security

The EU, as a global player and a community of values, should have a strategy to deal with new technologies as a part of its foreign and security policy. Only by synergizing trade, security and foreign policies, by aligning our values andinterests, can the EU fully leverage its power and act as a global player. The European Parliament has initiated such a strategy and has encouraged the European Commission and the European Council to adopt the recommendations.Overregulation would hurt and not help the potential of the open internet, yet in some areas rules need updating to adequately match the impact of technological developments and simultaneously establish adequate democratic oversight. In other areas, such as in redefining the European Neighbourhood policy, the momentum for realigning our interest and values should also include the role thattechnologies play. Knowledge sharing on accountability and the separation of powers in a rules and law-based society is a starting point. Additionally, twinningregulators can help develop mechanisms and oversight ensuring accountability as part of the transition that many MENA countries are going through.

Governments can not be effective on their own. Given the speed of technological developments, and to give a voice to different stakeholders, it is essential to promote structural collaboration between politicians, businesses, civilsociety and the public.

While there are serious challenges, the internet and technologicaldevelopments offer unprecedented opportunities for people to enjoy freedom, rights and developments. Digital freedoms, including uncensored access to information and communication, are indispensable enablers of traditional humanrights such as freedom of expression and freedom of assembly, and also for ensuring transparency and accountability in public life. Human rights violations can be documented and shared with the help of mobile phones. Additionally the opportunities for accessing knowledge and culture also have enormousopportunities for business development. The borderless nature of the internet underlines the need for an integrated approach incorporating freedom, security and opportunities. This should not become a zero-sum game.

This article was first published with Brill | Nijhoff publishers, and was featured on the Security and Human Rights Monitor (SHRM) website.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviervismarkt 4
2513 AM The Hague
The Netherlands

www.nhc.nl