EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

AFTER THE ARAB SPRING: NEW PATHS FOR HUMAN RIGHTS AND THE INTERNET IN EUROPEAN FOREIGN POLICY

DROI

EN

2012

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE UNION

DIRECTORATE B

POLICY DEPARTMENT

BRIEFING PAPER

AFTER THE ARAB SPRING: NEW PATHS FOR HUMAN RIGHTS AND THE INTERNET IN EUROPEAN FOREIGN POLICY

Abstract

Following the Arab Spring there have been numerous public debates about appropriate policy responses to events in the Middle East and North Africa (MENA). One of the largest public debates has centred on communications and the Internet and attempted to understand how EU policy could have prevented, mitigated or avoided some of the negative effects of Information and Communications Technologies (ICTs) during the Arab Spring. The following briefing paper provides an overview of the actions taken by governments in the MENA region to limit the positive impact of ICTs and the use of ICTs for harmful purposes. It then looks at key cases in the MENA region, analysing the events in Tunisia, Egypt, Syria, Libya and Bahrain before and during the Arab Spring. It then develops specific policy recommendations for European foreign policy, which are categorised by priority into short, medium, and long-term initiatives. In conclusion, it suggests that European policy makers have numerous avenues to develop policy solutions that could adequately respond to many of the issues raised during the Arab Spring, in the southern Mediterranean and beyond.

EXPO/B/DROI/2011/28 /July/ 2012

PE 457.102 EN

This briefing paper was requested by the European Parliament's Subcommittee on Human Rights.

AUTHOR:

Ben WAGNER, Researcher, European University Institute, ITALY

ADMINISTRATOR RESPONSIBLE:

Anete BANDONE
Directorate-General for External Policies of the Union
Policy Department
WIB 06 M 85
rue Wiertz 60
B-1047 Brussels

Editorial Assistant: Pia VANNESTE

LINGUISTIC VERSION

Original: EN

ABOUT THE EDITOR

Editorial closing date: 4 July 2012.

Printed in Belgium

ISBN: 978-92-823-3782-0
Doi: 10.2861/9556

The Briefing Paper is available on the Internet at
http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

If you are unable to download the information you require, please request a paper copy
by e-mail : poldep-expo@ep.europa.eu

DISCLAIMER

Any opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The events of the Arab Spring have proved highly challenging for policy makers around the world. Government interventions in the MENA region to massively restrict communications and to censor, surveil and control the communications of their citizens have been almost as widely publicised as the presumed positive effects of communications technologies to enable so-called 'Facebook revolutions.' While it should be clear that human beings and not technical devices create political change, the design and infrastructure of communications networks needs to consider basic human rights and fundamental freedoms in order to fully realise the potential of ICTs as an enabler of human rights.

The following document develops policy recommendations for appropriate responses of European policy makers to the Arab Spring and similar events in future. Surveillance and censorship of communications in the MENA region are not new and have been practised for decades. However renewed public interest has put a spotlight on these practises and increased transparency has demonstrated how utterly indefensible many existing practises are to European publics from an ethical and human rights-based perspective.

As a result the policy recommendations developed here have been categorised by the priority into short, medium and long-term initiatives. In the short term, this briefing paper recommends building structures, which enable the European Union to support telecommunications operators in critical situations. Numerous conversations with European telecommunications operators have suggested that their ability to resist calls to turn off the Internet is highly dependent on the level of external diplomatic support they receive. At the same time Europe also needs to develop a technical and diplomatic rapid response capacity to respond to situations like the turning off of Internet and mobile phone networks in Cairo swiftly. Finally there is an urgent need for stricter regulation of the 'worst of the worst' repressive technologies, which are explicitly designed to cause harm to human rights.

In the medium term, the EU should also consider developing effective regulation of dual use technologies, which are a separate category from the worst of the worst and exist in a far more complex regulatory space. It may also be possible to limit the demand for repressive technologies by actively supporting organisations promoting the democratic control of the Intelligence Services, Law Enforcement and Military Intelligence in third countries. Lastly, the EU should make all public sector funding, financial support and involvement in the creation of communications infrastructure conditional on basic human rights principles.

Commitments to such human rights principles in communications architecture would also seem an appropriate component of long-term European Foreign Policy. To illustrate what such human rights based principles might look like, the concept of Human Rights Based Communications Infrastructure (HRBCI) has been developed here and could form the basis for an on-going debate on these issues. As part of further long-term initiatives, there is a need to more actively innovate to promote human rights and ensure that existing publicly funded research and development (R&D) is guided by basic human rights principles. Finally, there is an overall need for a European body of knowledge that does not yet exist on how communications technologies may enable or harm human rights.

Any of these policy initiatives can actively contribute to improving the untenable status quo in Internet Foreign Policy at a European level. However the more of these initiatives can be implemented, the more effective an overall European Internet Foreign Policy Framework is likely to be in promoting human rights and mitigating harm. Such a framework is highly relevant in the aftermath of the Arab Spring in order to safeguard human rights in the 'post-Arab-spring-countries' and to be adequately prepared for similar events elsewhere.

1. BRIEF SURVEY OF ACADEMIC AND POLICY DISCUSSION

1.1 Action Taken by Governments to Minimise the Positive Impact of ICTs by Controlling, Monitoring or Shutting Down Communication Networks in MENA[1]

Communications networks in the MENA region have historically existed under close control of the state. Indeed such is the restriction of telecommunications and Internet networks in the MENA regions that a World Bank report identified it as one of the key factors hindering growth in the region (Terrab, Serot and Rossotto 2004) and scholars have noted that "telecommunications markets remain less open to competition than elsewhere in the developing world: competition is hindered, private participation is scarce and foreign ownership is most severely constrained" (Varoudakis and Rossotto 2004).

The same pattern could be observed on the Internet in Tunisia, one of the first countries in the MENA region where access to the Internet became available to the public in 1996. From the first stages of the development of the Tunisian Internet, extensive control and monitoring of the Internet was so pervasive that Tunisian Internet users served as guinea pigs for the products of the global censorship and surveillance industry (Chakchouk 2011). Moreover reports by the Open Net Initiative suggest that such practices were typical across the Middle East and North Africa (Noman and Zarwan 2007; Noman 2009) and countries from the region have featured prominently in Reporters Without Borders *Enemies of the Internet* list since it was first published in 2005 (RSF 2005).

Numerous different methods of censorship, monitoring, surveillance and control have been identified in recent decades. These include filtering emails, modifying and monitoring email traffic in Tunisia (Silver 2011) and pervasive censorship of the political websites in Bahrain (Noman 2009). Most of the countries in the MENA region engage in extensive telecommunications and Internet surveillance, although they have faced considerable challenges in doing so as the volume of phone and Internet traffic increased massively in the past decade.

In response to this challenge, various corporations – mainly from North America and Europe – became particularly engaged in supporting countries in the MENA region to monitor their citizens' communications. Civil society organisations that attended a trade show for industries, peddling these technologies, counted a total of 45 different government organisations from 15 countries in the MENA region, just for the period from 2006 to 2009. The organisations included Libyan State Security, Yemens National Security Agency, the Jordanian Armed Forces, Bahrain's Ministry of Interior and Sultan Kabous' Royal Court.[2]

It has been well documented that the vast majority of Internet censorship and surveillance technology employed in the MENA region stems from Europe and North America (Morozov 2011; Noman and York 2011; Silver 2011; Wagner 2012b). All the research that has been conducted so far on mobile telephone surveillance in the MENA region also indicates that the mobile surveillance technology is typically imported from North American and European vendors (Silver 2011; King 2011). At the same time censorship and surveillance technology are expensive to purchase and maintain and typically slows down Internet traffic (Chackchouk 2011).

[1] Parts of this report are based on an earlier report on *Exporting Censorship and Surveillance Technologies* for the Humanist Institute for Co-operation with Developing Countries (Hivos), which can be accessed here: http://www.hivos.nl/eng/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Exporting-Censorship-and-Surveillance-Technology

[2] A full list of government organisations from the MENA region can be found in Annex 2. The list is based on the *Surveillance Who's Who* by Privacy International, which can be found here: http://bigbrotherinc.org/v1/.

Admittedly outside technical assistance was also provided to human rights defenders (HRDs), activists, bloggers and other Internet users by various governments around the world. However it should be noted that the wider, positive impact of this external technical assistance is extraordinarily difficult to 'measure.' As a program manager in one of the oldest Internet freedom initiatives mentioned, "we are still discussing the appropriate metrics on how to measure it."[3] At the same time the number of Internet users using circumvention technologies in countries such as Egypt massively increased during public protests.[4] Similar patterns can be observed in early 2011 in other countries in the MENA region. Even if their effects are difficult to measure, there is clearly a demand for circumvention technologies from Internet users in the MENA region.

In part, these measurement difficulties exist because the money spent on such measures by governments is so extraordinarily small compared to the amounts spent on censorship, surveillance and control by governments in the MENA region. Moreover as public policy the field of external technical assistance to promote the positive role of ICTs through financial help or circumvention technologies is still extraordinarily 'young,' and many of the policies in this area remain under-developed.[5] Due to the relatively recent nature of these policy initiatives, the complex policy environment in which they are conducted and a general lack of reliable empirical data, it is hard to make reliable statements about what concrete impact external technical support has had.

Finally, shutting down telecommunications or Internet networks was not typically a strategy employed by states in the MENA region before widespread public protests in 2010 and 2011. Although heavy regulation of the media was common in the MENA region and the shutting down of specific television channels or media outlets was not uncommon, a complete removal of entire communications networks was an entirely new level of repressive authoritarian policies in the MENA region experienced in Egypt in 2011.

1.2 Development and Effects of Action taken by governments in the MENA region developed in 2010 and 2011 in the context of widespread public protests

Before looking at the effects of actions taken by states in the MENA region in 2010 and 2011, it is important to first consider that communications networks in MENA region were already repressive communications environments that were continually getting more repressive even before 2010. Countries in the MENA region were ramping up their repressive capacities, in response to the perceived danger of communications platforms and their extensive use for blogging and communication (York 2012). Even before the Jasmine revolution, Tunisia was preparing a new censorship and surveillance system specifically engineered for social networks. Before the Egyptian mass protests of 2011, in Tahrir Square, had even taken place, the Egyptian regime was already preparing an advanced Internet censorship system, technically similar to what was being used in Tunisia.

Ramping up repression of the Internet and telecommunications continued during widespread public protests in 2010 and 2011 across the MENA region. The measures employed often reflected the desperation of the bodies involved and were typically highly improvised. In Tunisia this involved hacking websites and defacing blogs of individuals engaged in the revolution. There are also numerous reports that government officials were stealing the access codes to Tunisian Facebook accounts in an

[3] Personal remarks made at Internet@Liberty, 23-24 May 2012, Washington DC.

[4] Further information is available here: https://blog.torproject.org/blog/recent-events-egypt

[5] The following workshop represents an early attempt at building greater comparative knowledge about the challenges such approaches face: http://www.intgovforum.org/cms/component/content/article/116-workshop-proposals/1046-igf-2012-workshop-proposal--no-112-evaluating-internet-freedom-initiatives-what-works.

attempt to deface or remove the Internet content these users were creating and to monitor their friends and contacts (Ragan 2011). In some cases technical means were used to steal usernames and passwords, however there are also many reported cases in which security agencies force prisoners to divulge their user names and passwords.

Of all governmental interventions in communications networks during the Arab spring, by far the most prominent remains the Egyptian government switching off the Internet for several days. As established in a *Joint Declaration on Freedom of Expression and the Internet* by the three rapporteurs on Freedom of Expression from the United Nations, Organization of American States and the African Commission on Human and Peoples' Rights and the Organization for Security and Co-operation in Europe Representative on Freedom of the Media: "[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified" (La Rue, Mijatovic, Botero Marino and Tlakula 2011).

At the same time, several other other important events during the demonstrations in Egypt are often forgotten, particularly the shutting down of the mobile phone networks in Cairo and the governmentally orchestrated SMS propaganda (Fossier 2012), which constituted part of an overall strategy to stem the tide of the revolution. What is however well documented is the extent to which European owned and controlled telecommunications operators participated in these events, with civil society accusing them of complicity in suppressing the Egyptian people at the behest of the Egyptian government (Access 2011). Interestingly conversations with large European telecommunications providers conducted after these events suggest that some had attempted to prevent their own complicity in these events. Had extensive and timely European diplomatic pressure been exerted, they might have been able to keep the Internet in Egypt and mobile phone communications in Cairo running for longer, or prevent them from being shut off at all.

Notably there is also a process of 'authoritarian learning' as the process of the Arab spring was on-going and different preferences and expectations structured different policy responses. Tunisia chose not to go as far Egypt in turning off entire communications networks although it certainly had the technical capacity to do so, while Egypt took a relatively 'brute force' approach to turning off the Internet. Libya – another country caught up in the Arab Spring that faced widespread public protests, responded by turning off the Internet in a more subtle manner. While much of the Libyan Internet was turned off, access to some government sites and a few key public portals was maintained, creating a highly controlled 'governmental Internet lite' (Dianotti et al. 2011).

This same 'Internet lite' was complemented with mass surveillance technologies for both telecommunications and Internet, the like of which few of the Western journalists who entered the Libyan Intelligence Services Surveillance Headquarters had seen before (Sonne and Coker 2011). The surveillance rooms were sealed shortly after the journalists had viewed them and Libya has since embarked on a different path for its future communications environment.

The same cannot be said for Syria. During the widespread demonstrations with terrible numbers of fatalities in 2011, the Syrian regime decided to augment its already highly repressive Internet surveillance infrastructure with an additional layer of Internet surveillance. Unable to do so alone, it paid for the services of a consortium of European technology companies to install a new Internet surveillance system. Faced with widespread public pressure following the publication of their work in international media and the threat of their equipment being included in impending European sanctions, the consortium of European technology companies pulled out of Syria and repressive communications technologies were later included on the European sanctions list.

As the Tunisian, Egyptian, Libyan and Syrian examples show, there is a large market for repressive ICT technology, even or perhaps especially during revolutions. Indeed it seems that some ICT vendors market some of the 'worst of the worst' ICT technologies to dictators in crisis, hoping for high margins in supporting authoritarian regimes repressing their people during revolutions. Importantly the market for ICT technology used to repress MENA populations is dominated by European and North American companies. The vast majority of repressive technology, systems and services used in communications networks in the MENA region is/seems to be coming from Europe and North America.

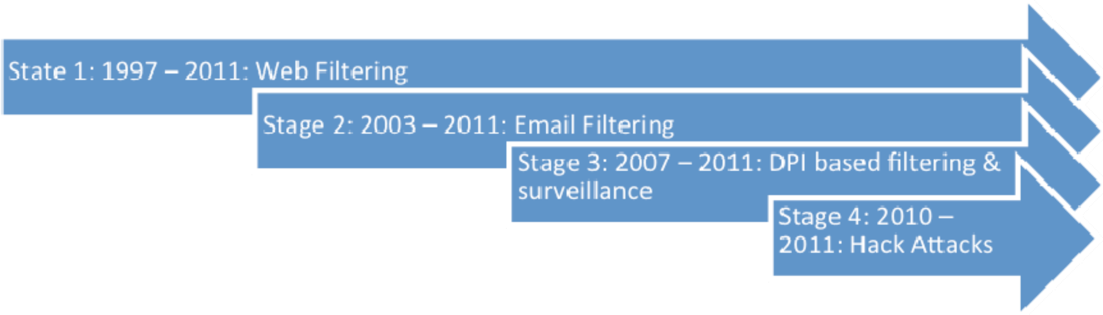
2. ANALYSIS OF KEY CASES IN THE MENA REGION

2.1 Tunisia

The Arab Spring begun in Tunisia and without the extraordinary events that took place in this small country, the Middle East and North Africa would not be the same today. The Jasmine Revolution in Tunisia sent shock waves across the MENA region and began a process, which has since become known as the Arab Spring.

Tunisia was one of the most conspicuous examples of the use of communications technologies to restrict human rights. It featured prominently on Reporters Without Borders *Enemies of the Internet* list for many years in a row and the Tunisian government was in most cases the first country in the region to begin using communications surveillance, censorship and control technology. Moreover it seems that the Tunisian Government had cut side-deals with vendors of such technologies, offering their citizens as guinea pigs for new human-rights-harming technologies in exchange for lower prices (Chackchouk 2011).

The following graph provides a broad overview of the development of Internet filtering in Tunisia and its development over the years. It shows how additional layers of technical filtering were added to the overall censorship infrastructure over time:


State 1: 1997 – 2011: Web Filtering
Stage 2: 2003 – 2011: Email Filtering
Stage 3: 2007 – 2011: DPI based filtering & surveillance
Stage 4: 2010 – 2011: Hack Attacks

[6]

This censorship covered several different channels of Internet communications, initially simply filtering lists of websites, then moving on to emails and eventually filtering individual Internet packets. These efforts culminated in a targeting of specific individuals, whereby personal user accounts and public websites were hacked. Notably most of the repressive technology systems were developed with support from European and American companies (HL Deb, 21 November 2011, c210W; Silver 2011).

What should also become evident is that the infrastructure of Internet censorship began long before the Arab Spring in Tunisia and was an integral part of Internet communications in Tunisia. Indeed the

[6] Wagner, B. (2012). Push-Button-Autocracy in Tunisia: Analysing the role of Internet Infrastructure, Institutions and International Markets in Creating a Tunisian Censorship Regime. *Telecommunications Policy*, *36*(6).

entire Tunisian Internet was constructed to allow interference and the harming of human rights. Internet architecture was centralised and the role of the private sector was severely limited in order to ensure that the regime had maximum control over Internet communications.

Separately from censorship, communications surveillance was equally rampant both on the Internet and in mobile and fixed line telecommunications. Tunisie Telecom as well as private ISPs and mobile telecommunications operators were required to support the state in its efforts to surveil its citizens. Similar to Internet censorship, communications surveillance became more advanced over time, as successive layers of repressive technology were added to communications networks.

During the revolution in Tunisia levels of censorship, surveillance and Internet control were progressively increased. As part of his last desperate concessions before he fled the country only days later, Ben Ali agreed to remove all censorship and institute a free press. Within hours this decision was implemented and Tunisians were suddenly able to access many sites that were unable to access before.

However much of the infrastructure of censorship and surveillance is still in place in Tunisia. Following the Jasmine Revolution it remains to be seen to what extent the new political space in Tunisia may enable more fundamental changes. Existing repressive infrastructure is a legacy of the authoritarian past that poses challenges for Tunisia's hopeful political future. It will require considerable political will in Tunisia and support from other actors in Europe and elsewhere to rid itself of this legacy. For a country that had one of the most repressive Internet infrastructures in the world, the country has come a long way, but it still has work to do if the ideals of the Jasmine revolution are to be realised.

2.2 Egypt

The swift success of the Jasmine Revolution in Tunisia entirely changed the opportunity structure for societies across the MENA region. Seeing the change that had been possible in Tunisia led to widespread protests across the MENA region, with Egypt as one of the first countries where mass public demonstrations took place.

Unlike Tunisia however, Internet censorship in Egypt was far less restrictive than was the case in Tunisia (Deibert et al. 2010). When restrictions of freedom of expression took place on the Egyptian Internet, these were not a product of Internet filtering, but rather of more general surveillance. Both bloggers and print journalists alike, who were identified as overstepping what the Egyptian establishment perceived as 'red lines', were arrested and detained, often for indefinite periods of time without trial (HRW 2010).

Instead of building an Egyptian censorship infrastructure, the state has focused on a broad surveillance network across communications mediums. This was done in close co-operation with an American technology developer and a local technology integrator, who built Internet surveillance systems in Egypt and exported them across the MENA region (Karr 2011). Telecommunications technology was equally subject to extensive surveillance, but it was only during widespread public protests in Egypt that the restriction of communications in Egypt received worldwide public attention.

The Egyptian attempt to control various forms of communications came to a head during widespread public protests in early 2011. While it has become common knowledge that Egypt 'switched off' the Internet for several days in January 2011, the precise nature of manipulation of communications is seldom discussed in greater detail. Not only was the Internet turned off across Egypt and propaganda SMS were forcibly sent out by the regime before turning off the entire mobile phone network in Cairo (Fossier 2012).

According to credible reports these steps were taken by local mobile telecommunications operators under direct threats of force by the Egyptian military directed at local staff (Fossier 2012). While these local operators did consult with their corporate headquarters in Europe, they saw little alternative but to do the bidding of the military. This is particularly the case as the military also had the ability to ask power companies to remove the power supply from mobile telecommunications operators, which would have had the same effect of turning off the network but at a far greater cost to the mobile operators (Fossier 2012).

At the same time mobile phone operators have come under considerable pressure for their complicity in supporting the regime in its actions (Access 2011). Particularly considering the legitimate concerns of civil society and human rights advocates, there seems to be some space to develop initiatives, which promote human rights in this context. The strong linkage of many telecommunications operators in the MENA region to Europe is as evident in Egypt as it is in Tunisia. This linkage should not be a competitive disadvantage for European telecommunications operators. Instead they should be supported more strongly in their attempts to avoid complicity and should be provided with additional support in crisis situations.

In Egypt, the fall of former President Mubarak was just the beginning of a downward spiral into a continually more repressive communications environment. Since then the military authority SCAF has intensified detentions of bloggers and journalists and there have been continuous reports in 2011 and 2012 of manipulations of mediums of communication with a strong focus on the Internet (RSF 2012). Both in regard to the new communications environment and more generally in Egypt after the fall of Mubarak, the future of human rights is looking increasingly bleak.

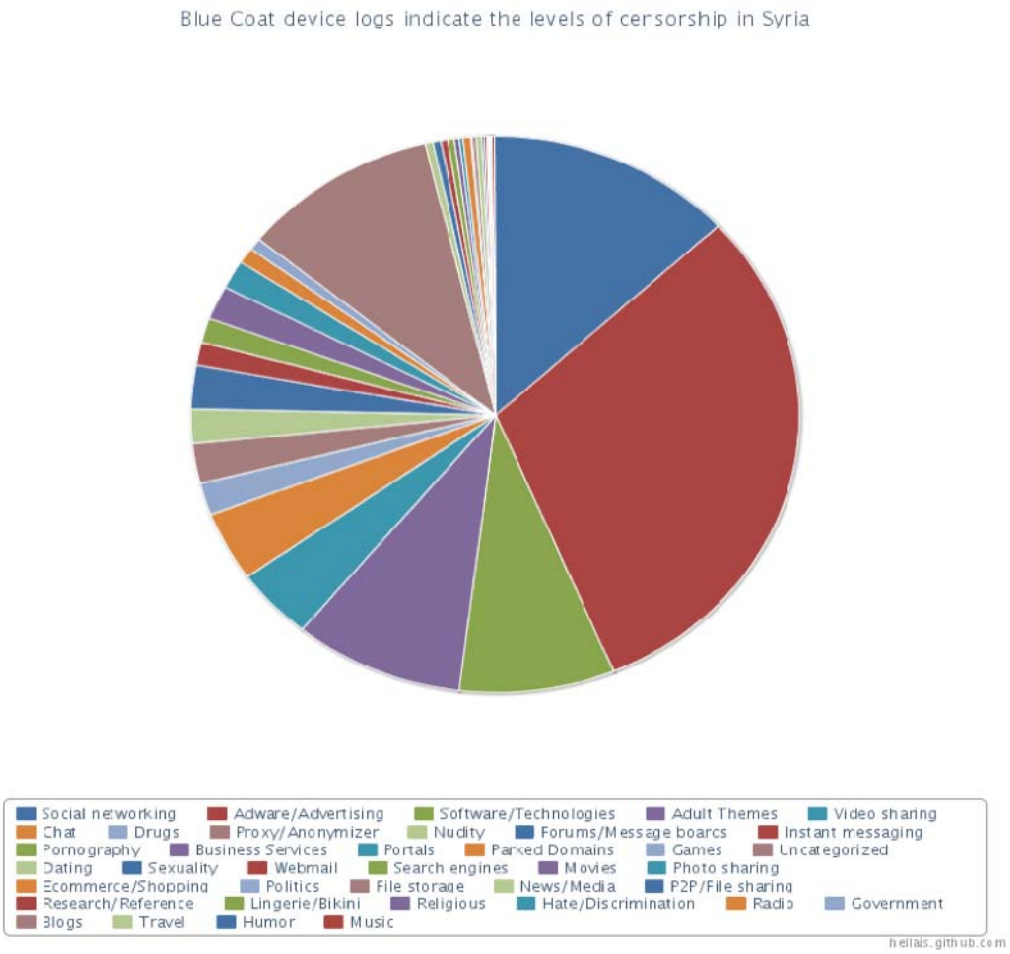
2.3 Syria

Another country inspired by the success of the Jasmine Revolution in Tunisia is Syria, although hopes of a similar success of non-violent protests have been marred by thousands of dead and severely injured Syrians in terrible circumstances. With increasing accusations of war crimes and reports of the terrible violence (HRW 2012b) it is impossible to discuss the communications environment in Syria outside of this context.

Communications media have historically been severely restricted in Syria, with censorship and surveillance rife (Deibert et al. 2010). However in contrast to the similarly restrictive regimes in the region, the Syrian Internet architecture is far less developed than in countries such as Tunisia. This means that slow and under-developed Internet architecture is further limited and slowed down by additional layers of censorship and control.

Additionally telecommunications and Internet surveillance are used to target specific activists and bloggers who are considered particularly dangerous. These are then detained or imprisoned as part of a wider regime strategy to limit political expression and intimidate human rights defenders and political activists (Sutton 2012). The extent to which the Syrian government was surveilling its citizens became apparent when the global hacker community discovered that many of the North American Internet surveillance devices on the Syrian Internet were entirely insufficiently protected (Filastò 2011).

This led to an astonishing amount of data being published from North American Internet surveillance devices within Syria, which demonstrates the extent to which the regime was studying the actions of its citizens. The graph below is a graphical overview of the data that was published:



[7]

Not content with this incredible amount of data it had already collected on its citizens, the Syrian government embarked on an even more ambitious project to increase the level of surveillance in Syria further still. The system was custom built by a consortium of European companies from Italy, France, Germany and also included North American technology (Elgin and Silver 2011). Together their more advanced system would have allowed for an additional "crackdown on protests" (Elgin and Silver 2011) and an even greater violation of Syrian citizens human rights.

Worryingly from a corporate social responsibility perspective, the companies engaged in the consortium were building this system during extensive public protests and widespread violence in Syria. It seems hard to believe that none of these corporations had any knowledge of the ongoing political situation, or that they were unaware how the system they were building in Damascus would be used.

The public outcry that followed the publication of investigative reporting about the complicity of European companies in supporting the Syrian regime eventually led the consortium to pull out of Syria in November 2011 (Elgin and Silver 2011). At the beginning of December, the Council of the European Union passed additional sanctions, to specifically restrict "equipment and software intended for use in the monitoring of the Internet and telephone communications" (17985/11) from entering Syria.

[7] Filastò, Arturo. 2011. "Blue Coat device logs indicate the levels of censorship in Syria." Retrieved from http://hellais.github.com/syria-censorship/.

Apart from showing the insatiable appetite of repressive regimes for technologies to surveil their populaces, this episode demonstrates that there is a marketplace for revolutions in which companies specifically offer their services to countries already suffering widespread human rights violations. Similar corporate actions could be observed in Egypt, where one company specifically offered additional surveillance capacity to the Egyptian government because of the widespread protests. Such corporate interventions cannot be reconciled with basic human rights standards and it seems unlikely that self-regulation would have any kind of effect in either of these contexts.

2.4 Libya

Another country to witness widespread public protests following the Jasmine Revolution in Tunisia is Libya. However like Syria, non-violent protests were quickly marred by bloodshed and the resulting conflict led to tens of thousands of deaths in Libya and a humanitarian crisis whose repercussions continue to this day (HRW 2012a).

Despite a highly questionable human rights record, Internet access in Libya seems to have been relatively unrestricted until 2011 (Deibert et al. 2010). This does not mean however that it was not extensively surveilled, with surveillance technology from North America built into the network (Karr and Le Coz 2011). However it is only after the revolution that a broader picture of what Internet surveillance took place is being published (Sonne and Coker 2011). The Libyan Internet surveillance systems involved technology from companies not only in North America, but also from Europe, with one French company providing surveillance technology.

What is notable in Libya is that European companies were openly selling technologies to the regime that went far beyond even highly invasive lawful interception technologies. One glossy European brochure of the technologies used in Libya described this as the shift "from Lawful to Massive Interception" (Aikins 2012). Exporting these systems has drawn widespread criticism from human rights groups and has recently become the subject of a court case in France, which accuses a French company of "complicity in acts of torture in Libya" (Sonne and Gauthier-Villars 2012).

Following the Egyptian example, Libya also decided to 'turn off' the Internet in the country during extensive public unrest in 2011 (Cowie 2011). However rather than completely blocking all forms of Internet communications, the country allowed traffic to certain government sites to pass while blocking access to others (Dianotti et al. 2011). This more nuanced approach can be seen as another stage in the development of such repressive techniques as part of a wider learning process between authoritarian regimes in the region.

2.5 Bahrain

Bahrain is another country in the MENA region, where extensive censorship, surveillance and control of communications are in place. Both the Internet and telecommunications were extensively surveilled, while the Internet was subject to numerous forms of censorship (Deibert et al. 2010). Although the country has a very high level of Internet penetration and prides itself on being one of the leading hubs of technology in the region, citizens' access to these technologies is highly restricted.

On the Internet this restriction of individual rights to seek, receive and impart information has historically taken place in close co-operation with Western companies. It has been well-documented that the North American Company SmartFilter provides the 'filtering lists' based on which the Bahraini System of restriction of Internet content operates (Noman and York 2011).

At the same time several German companies have provided Bahrain with surveillance technology, which allowed them to identify human rights defenders and activists. Journalists who established that these technologies were being used to surveil Bahraini citizens also discovered that those citizens had been tortured as a direct result of the use of these surveillance technologies, while the authorities read out "several pages of transcripts of his text message" (Silver and Elgin 2011).

Importantly the targeting of political activists and human rights defenders has increased considerably since the widespread public protests in Bahrain in 2011. Not only has the number of incidents of serious human rights abuses increased, but also the types of abuses have got progressively worse (Mepham 2012). These abuses are closely linked to surveillance technology, which is often used to identify Bahraini citizens and thereby enable human rights abuses.

3. COURSES OF ACTION FOR THE EUROPEAN UNION

The previous overview of the current debate and the analysis of the widespread public protests in the Middle East, North Africa in 2010 and 2011 should give some indication of scale of the issue being discussed. The role of the European Union in these events has been gradually increasing, but the EU has yet to develop a coherent policy response.

The following policy recommendations are an attempt to start a dialogue on how the European Union might move towards a coherent policy framework on these issues considering short, medium and long-term perspectives. In order to do so there is a need to first consider existing EU policy responses, where the European Union has policy leverage and how this leverage can be implemented.

3.1 Existing European Policy Responses

As events unfolded across the MENA region, there were numerous responses by HRVP Ashton, emphasizing that the EU is "firmly opposed to any unjustified restrictions of access to the internet and other new media" (EU11-069EN, CL11-006EN, A 010/11, A 016/11, P7_TA(2011)0038). Events in Egypt were cause for particularly concern, with MEPs calling HRVP Ashton to "reach out to European companies […] to urge them not to be complicit in the Egyptian black hole" (Schaake 2011).

In March 2011, the European Commission and the High Representative of the Union for Foreign and Security Policy presented their *Partnership for Democracy and Shared Prosperity with the Southern Mediterranean* (COM(2011)200). This European strategy has become the foundational document for European initiatives in this area and is based on three key elements:

- "democratic transformation and institution-building, with a particular focus on fundamental freedoms, constitutional reforms, reform of the judiciary and the fight against corruption
- a stronger partnership with the people, with specific emphasis on support to civil society and on enhanced opportunities for exchanges and people-to-people contacts with a particular focus on the young
- sustainable and inclusive growth and economic development especially support to Small and Medium Enterprises (SMEs), vocational and educational training, improving health and education systems and development of the poorer regions" (COM(2011)200, 3).

The strategy also describes the immediate response of the EU, including humanitarian aid and visits of HRVP Ashton to Egypt and Tunisia. In regards to communications technologies, it includes several paragraphs which are particularly interesting in this context:

> "The use of electronic communications technologies - on top of satellite broadcasting - greatly facilitated the wave of upheavals in the Mediterranean countries. The widespread use of mobile phones combined with social networking via Internet - showed the importance of information society tools and technologies to the circulation of information. In countries where the circulation of information is partially restricted such tools can greatly contribute to the democratisation of societies and the creation of public opinion through the promotion of freedom of expression.

> While some regulatory reforms have been undertaken, in many of the southern Mediterranean countries the regulatory environment is still insufficiently developed to exploit the full growth and productivity potentialities of the Information and Communications Technology sector. The main critical factors which remain to be addressed are the creation of truly open markets (which often remain quasi monopolies), the establishment of independent regulators, the creation of a level playing field and of competitive conditions for market players, efficient management of spectrum and safeguards of users' privacy and security.
>
> Moreover, ensuring the security, stability and resilience of the Internet and of other electronic communication technologies is a fundamental building block in democracy. It is necessary to avoid arbitrarily depriving or disrupting citizen's access to them. Given the trans-border and interconnected nature of electronic communications technologies, including the Internet, any unilateral domestic intervention can have severe effects on other parts of the world. The Commission will develop tools to allow the EU, in appropriate cases, to assist civil society organisations or individual citizens to circumvent such arbitrary disruptions" (COM(2011)200).

In many regards, this document can be seen as a roadmap for future EU policies in this area. It is in this context that decision of the Council of the European Union to restrict exports of surveillance technologies to Syria in December 2011 can be understood (17985/11).

The Partnership for Democracy and Shared Prosperity is also the basis for the No Disconnect Strategy as developed by EC VP Kroes (IP/11/1525). The strategy is based on four pillars:

- **"Developing and providing technological tools** to enhance privacy and security of people living in non-democratic regimes when using ICT.
- **Educating and raising awareness of activists about the opportunities and risks of ICT.** In particular assisting activists to make best use of tools such as social networks and blogs while raising awareness of surveillance risks when communicating via ICT.
- **Gathering high quality intelligence about what is happening "on the ground"** in order to monitor the level of surveillance and censorship at a given time, in a given place.
- **Cooperation.** Developing a practical way to ensure that all stakeholders can share information on their activity and promote multilateral action and building cross-regional cooperation to protect human rights." (IP/11/1525)

The European Parliament has also played an important role in this process. It has increased export restrictions by ensuring that there can be no blanket exemptions for dual-use goods which can be used to harm "human rights, democratic principles or freedom of speech" (EP: P7_TA-PROV(2011)0406). The EP has also pushed for Internet freedom funds in the European Instrument for Democracy and Human Rights (EIDHR) and given Internet freedom and the regulation of surveillance technologies a prominent role in the *European Parliament resolution of 18 April 2012 on the Annual Report on Human Rights* (P7_TA-PROV(2012)0126).

This EP resolution argues for mandating "accountability for EU-based companies, in order to improve the monitoring of the export of products and services aimed at blocking websites, mass surveillance, monitoring all Internet traffic and (mobile) communications, breaking into private conversations and transcribing them, filtering search results, and intimidating Internet users including human rights defenders" (P7_TA-PROV(2012)0126). The European Parliament has also appointed Marietje Schaake MEP (ALDE/NL) as the first EP-Rapporteur for a European Strategy for Internet Freedom. Ms Schaake has been one of the most important voices on these issues and is in the process of preparing a parliamentary report on *European Strategy for Internet Freedom in the World* for the Committee on Foreign Affairs (AFET).

At the same time it is important to note that none of these strategies are developed in a political vacuum. There is an on-going debate among EU policy makers whether to develop siloed 'cyber'-

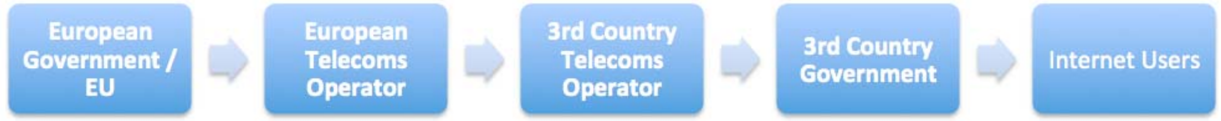
strategies within which human rights, cyber-security and economic and social development are tackled separately, or whether to develop overarching ‘cyber’-strategies, which integrate all three elements. Although a siloed approach has been typical until relatively recently, current developments suggest that the EU may by moving towards a more joined up approach. The EU Food-for-thought Paper from October 2011 is an example of such an approach and - while mentioning human rights – it places a strong emphasis on safety and security on the Internet (HOME/INFSO/EEAS/A2/MAH(2011)). While EU policy coherence in Internet or ‘cyber’ policy and governance has been emphasized much of late, it must be ensured that “achieving greater policy coherence” (11855/12) contributes to promoting and safeguarding human rights.

It is unclear to what extent these developments will affect the ongoing development of the No Disconnect Strategy or related EU policy measures in this area. HRVP Ashton has repeatedly suggested that human rights run through EU foreign policy like a “silver thread” (SPEECH/10/317). At the same time many MEPs have questioned whether this is actually the case, with the Chair of the EP Subcommittee on Human Rights suggesting that she is still “[w]aiting for the ‘silver thread’ to become visible and credible” (Lochbichler 2011). In this context it can only be hoped that human rights are not lost within integrated cyber-strategies but do indeed become the ‘silver thread’ for European Internet Foreign Policy strategies.

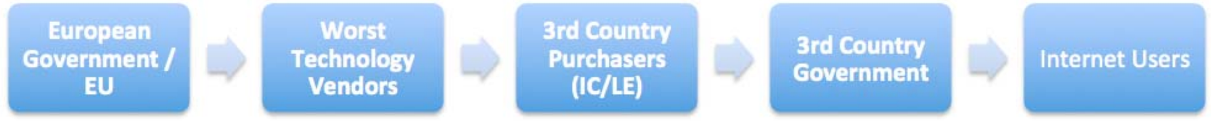
3.2 European Policy Leverage and Global Supply Chains

The European Union has a strong position in global Telecommunications markets. Together with North America, Europe controls a substantial proportion of supply and demand in both telecommunications and Internet markets. This market position gives European Policy in this area, particularly when conducted in concert with North America, considerable leverage in the global telecommunications and Internet markets.

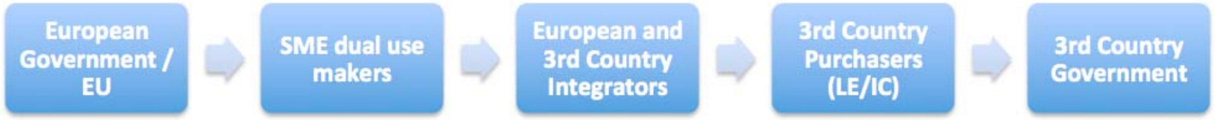
There is no question that joint efforts by European and North American telecommunications equipment manufacturers and telecommunications operators could be extraordinarily effective. However as the two groups have different roles and interests within the market, it is important to differentiate between them. The first graph shows a simple map of policy linkages for European telecommunications operators:



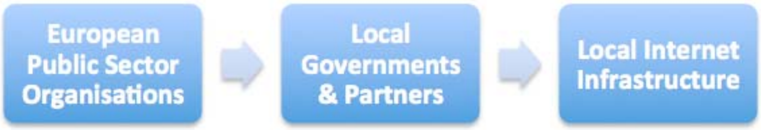
By contrast, manufactures of telecommunications equipment makers are often required to integrate control mechanisms into their products. These range from lawful intercept provisions through to intelligence services and military customers.



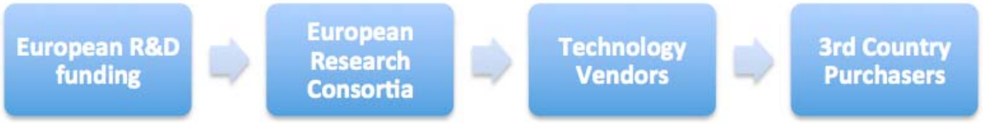
Then there are a small group of companies who explicitly develop technologies designed to harm individual human rights. These companies represent the ‘worst of the worst’ in terms of their human rights impact on the Internet and are explicitly designed to provide censorship and surveillance to organisations operating outside the rule of law and democratic oversight.


European Government / EU
SME dual use makers
European and 3rd Country Integrators
3rd Country Purchasers (LE/IC)
3rd Country Government

At the same time European and North American development organisations as well as International Organisations fund a considerable part of the telecommunications and Internet infrastructure in the world. Following the Paris Declaration and the Accra Agenda for Action, many aspects of development policy have become conditional on meeting specific criteria and embedded in evaluative processes (OECD 2008). The basic political linkages in this process are displayed relatively simply here:


European Public Sector Organisations
Local Governments & Partners
Local Internet Infrastructure

Finally, Europe is one of the leading global players in research and development into telecommunications and Internet devices, services and infrastructure. Much of this research is funded by the European Union and its member states. This leads to the following graph of simplified policy linkages in regard to research funding in telecommunications and creating Internet infrastructure:



3.3 Short Term European Policy Initiatives

In order to analyse where European Union policy can be most effective, it is first necessary to look where the greatest impacts can be achieved. In the short term it would seem reasonable to focus on specific goals, which can be implemented within 12 months. Following the lessons of the Arab Spring, the following three initiatives would seem most urgent:

- Support European telecommunications operators promptly in order to prevent, slow down or mitigate the turning off of the Internet in third countries.
- Develop a European rapid response capacity to provide a technical and diplomatic response to urgent threats to human rights on communications networks in third countries.
- Use sanctions, export controls and other policy mechanisms to prevent the 'worst of the worst' human rights invasive technologies getting into the hands of repressive regimes.

3.3.1 Supporting European telecommunications operators in critical situations

One of the defining events of the Arab Spring was the 'turning off' of the Internet in Egypt and of telecommunications networks in Cairo. While this demonstrated to the world how vulnerable communications networks may be to state interference and how eager repressive regimes may be to exploit this, it also led to an on-going debate about corporate complicity in supporting repressive regimes during revolutions.

In public, many of the European telecommunications operators involved in the events in Cairo stated that they were unable to do anything, suggesting that their staff were threatened with military force and that they feared for the lives of their staff (Fossier 2012). Notably some of these organisations have also suggested that nobody in their organisation could foresee a situation like Egypt and that their internal decision making procedures were unprepared for such events.

There have also been suggestions – such as from Larry Stone, president group public & government affairs at BT - that telecommunications operators may wish to engage in human rights and the Internet scenario-planning during any regular corporate crisis management planning exercises. These exercises will however need to reflect the risk profiles of individual companies, their various business models and geographic footprints. He added that it is likely that many major ICT companies engage in regular such top level exercises around major risks affecting their organisations and that the sorts of issues in the human rights and the Internet could fall within the ambit of such exercises going forward, perhaps involving a number of stakeholders, and could offer valuable experience and ideas.[8]

Having consulted with several large telecommunications operators in Europe who own and operate Internet and telecommunications services in the MENA region, all have suggested that their internal decision making processes in such situations are heavily dependent on external support. Indeed some of the individuals went as far as saying that their course of action in these situations was dependent on their ability to receive support from the European national government where their headquarters is based. Consequently it seems entirely reasonable to support European telecommunications operators, their subsidiaries and their respective employees to 'do the right thing' in countries outside of Europe.

A central point of contact should be provided at a European level providing telecommunications operators with timely advice and support in these situations. What is challenging in this context is responding quickly and effectively to external pressure to shut down or misuse communications networks, particularly if a European response needs to be escalated swiftly to higher levels of policy making. At the same time on-going conversations with European telecommunications operators have suggested that effective advice and a swift response could be highly effective in preventing similar situations to those witnessed in Cairo and Egypt from happening again.

3.3.2 Develop a European technical and diplomatic rapid response capacity

Closely linked to a central point of contact for European telecommunications operators is the development of a rapid response capacity. While a rapid response is also important for a central EU point of contact, there are other aspects to a rapid European response that need to be considered. These relate to both technical and diplomatic responses to events in third countries, which require a coordinated European response and go beyond supporting European telecommunications operators.

Developing technical rapid response capacity may provide the most immediate response to events on the ground in an attempt to ensure that any disconnection from or substantial disruption of the Internet in third countries finds an appropriate response. This may be both through ensuring citizens in third countries have alternate means to access the global Internet directly, or by providing them with technologies to circumvent the limitations of their existing connection. In both cases any response must be sufficiently prepared, closely coordinated with existing civil society initiatives and oriented towards upholding the human rights of citizens in third countries.

However it is crucial that a diplomatic rapid response capacity is developed together with a technical rapid response capacity. This is both in response to potential diplomatic friction that technical rapid responses may cause and to provide a rapid response in the many cases in which a technical response is

[8] Personal communications with Larry Stone, President of Group Public and Government Affairs at British Telecom on 23.05.2012.

inappropriate, insufficient or ineffective. The events of the Arab Spring suggest that timely diplomatic intervention on these matters may assist in mitigating the negative effects on human rights in third countries.

At the same time a rapid response capacity developed at a European level can only be effective if linked to the existing initiatives in this sphere. This refers to both diplomatic initiatives on Internet Freedom such as the 'Freedom Online Coalition' of 15 states launched in Den Haag[9], private-sector led initiatives on corporate social responsibility such as the Global Network Initiative and civil society initiatives by the Electronic Frontier Foundations, Telecomix or TacticalTech. While there a surely many more initiatives that could be named in this context, it is essential that Europe engages with the existing 'players' in this space rather than attempting to act alone or reinvent the wheel.

A rapid response capacity cannot be the single panacea for supporting human rights on the Internet, but it may serve to mitigate harm in crisis situations. As such it may serve as a first step to developing an overall European strategy in this area, which will require close co-operation between the respective DGs of the European Commission, the EEAS, relevant European Council Working Parties including COHOM & RELEX and the European Parliament. Such close co-operation will take some time to develop and will also need to consider the roles and responsibility of new or existing Interservice Groups. But - as European responses to the situation in Syria have shown - they can be effective and should be developed further to deal with events far beyond the MENA region.

3.3.3 Prevent the 'worst of the worst' technologies getting into the wrong hands

There is a market for revolutions. Without the knowledge of many European policy makers or citizens a small group of technology makers has grown swiftly in the last few years. These small groups of companies engage specifically in selling technologies which are created to be human rights invasive, particularly in countries which lack basic human rights protections.

To make matters worse, some of these companies specifically market their technologies to countries in the middle of widespread public protests and revolutions. Egypt and Syria are just two examples of countries where highly invasive technology was offered to regimes in times of crisis. These are the same companies, which also celebrated their 'naming and shaming' in international reporting on their complicity in human rights abuses. When companies wear their invasion of human rights as a badge of honour at international trade shows, it should be patently obvious that any attempt at self-regulation is likely to be ineffective.

Indeed anything less than a far stricter control regime created and enforced by the European Union and its member states is likely to be ineffective. As many of these companies currently engage in 'hopping' between different European jurisdictions in order to exploit various loopholes within European legal jurisdictions, a pan-European approach is likely to be particularly effective, as is co-operation with European partners in the context of the Wassenaar Arrangement.

Such a control regime would need to consider export controls as a first component of the regime, together with the development of 'worst of the worst technology' sanctions lists for specific high-risk countries. It would also need to update these lists on a regular basis as part of a regular review process

[9] The Final Declaration of the Freedom Online Conference in Den Haag can be found here and has been endorsed by Austria, Canada, the Czech Republic, France, Estonia, Ghana, Ireland, Kenya, Mexico, Mongolia, the Netherlands, the United Kingdom, the United States, and Sweden, who all consider themselves members of the Freedom Online Coalition: http://www.minbuza.nl/en/ministry/conference-on-internet-freedom/final-declaration-coalition-freedom-online.html Costa Rica later joined the Freedom Online Coalition in May 2012.

to ensure they reflect the 'state of the art' of the worst of the worst technologies. However the history of export control and sanctions regimes in Europe has repeatedly shown their weakness as a tool of policy, as well as their frequent permeability. Consequently additional policy tools will be necessary to ensure that the 'worst of the worst' technologies do not fall into the wrong hands. One policy mechanism stands out here as an obvious driver of effective European policy: transparency.

In Syria, it was the hard work of investigative journalists and civil society - particularly Vernon Silver from Bloomberg and Eric King from Privacy International - that brought the sale of surveillance technologies during on-going public protests and human rights abuses in Syria to the attention of global publics. The effect of putting this information in the public domain led European companies involved to pull out of Syria and the European Union to add these kinds of technologies to the sanctions lists on Syria. Creating institutionalised transparency for the trade in and export of these kinds of technologies at a European level could have similar positive effects, particularly if the documents were provided to European publics in a swift and timely manner. Greater transparency may also allow European citizens and civil society to respond more effectively. One example of such a response is a French court case about corporate complicity in torture in Libya following widespread publication of the involvement of a French company (Sonne and Gauthier-Villars 2012).

Separately from enforcing transparency, much stricter export regulations of surveillance equipment across Europe have to be imposed, as a necessary component of regulating the trade in surveillance technologies. Here the Privacy International *Briefing: British exports of surveillance technology to repressive regimes* may serve as an excellent template for both member states and the EU to develop the debate further.

One path for such regulation may include the targeted financial sanctions against companies selling the worst of the worst technologies, such as those outlined by the White House for Iran and Syria in an Executive order on April 23 2012.[10] While these sanctions will only be effective for two countries, the psychological effect of potential bank account seizures for surveillance technology exporters will likely be far greater. Targeted financial sanctions are likely to serve as a model in cases where harm to human rights is likely and a swift urgent response is necessary.

By focusing on the ''worst of the worst' technologies, which are typically single use technologies specifically engineered to harm human rights, the European Union can take an important first step towards mitigating harm to human rights in third countries. Moreover it will encourage larger European companies to distance themselves from these kinds of business models and encourage a broader public and policy debate on where to draw the line for dual use technologies.

Any such regulation of technology must be mindful to ensure that they do not harm individual or business access to technologies that are essential for the operation of communications networks. Nevertheless, the current status quo is evidently unacceptable to European publics and policy makers and anything less than 'hard' regulation will be ineffective in stemming the flow of the 'worst of the worst' technologies to repressive regimes.

3.4 Medium Term European Policy Initiatives

Moving from short term to medium term policy initiatives that can reasonably be implemented within 12 to 36 months, there are several equally important policy initiatives that require a greater length of

[10] For further details about the executive order issued by the White House on 23 April 2012 see http://content.govdelivery.com/attachments/USTREAS/2012/04/23/file_attachments/108232/2012iransyria.eo.rel.pdf

time before they can be implemented. This does not make the measures any less important, but it does mean that their implementation will require a greater period of time. These initiatives are:

– Developing effective European regulation of dual use technologies in close co-operation with all relevant stakeholders.

– Supporting the democratic control of the intelligence services, law enforcement and military intelligence in third countries.

– Make European financial support and development funding for communications infrastructure conditional on its capacity to support human rights.

3.4.1 Develop effective European regulation of dual use technologies

Having discussed the far clearer category of the 'worst of the worst' technologies, it is also important to discuss the 'greyer' field of dual use Internet technologies. It is often very difficult to ascertain to what extent technologies, systems and services provided by European companies and their international subsidiaries may be harming human rights. Particularly European companies producing telecommunications and Internet infrastructure have had to learn this the hard way in the last years, as they have been targeted by numerous public campaigns for doing business with repressive regimes.

As such it is encouraging when a large European supplier of telecommunications hardware and Internet infrastructure publicly states that they have "realised through [their] experience that the traditional industry position that we as a company only deliver technology but that we have no responsibility for how our technology is being used is not acceptable any more" (NSN 2012). Such statements mark the beginning of a long overdue debate on the role of telecommunications hardware and Internet infrastructure providers in enabling or harming human rights. In response to this challenge several large European companies have developed early drafts of human rights guidelines and a joint industry initiative has even sprung up.

For such initiatives not to remain 'self-regulatory fig leaves', they will require extensive involvement both by the public sector, civil society and other relevant stakeholders. Some companies have tended to prefer 'coffee cup consultation' to actual substantive engagement with relevant stakeholders. Despite the important role of other stakeholders, the burden is evidently still on the manufacturers of telecommunications hardware and Internet infrastructure to demonstrate that they are adhering to processes to fulfil their responsibility to 'do no harm' to human rights and to avoid complicity in doing so.

There is an important role to be played here by the self-regulatory stakeholder guidance for the ICT sector being developed for the European Commission by the Institute for Human Rights and Business and Shift (IHRB 2012). However it should be clear to all stakeholders involved that self-regulation alone will be a first, but insufficient step on the path towards developing appropriate policy responses to the danger of human rights abuses being enabled by dual use technologies.

As discussed at length above in regard to the 'worst of the worst' technologies, transparency can play an important role in regulating dual use technologies. Simply by publicising applications for permission to export technologies, the level of transparency and overall knowledge about the European trade in these technologies can be substantially increased. This could be highly effectively when linked to ex ante procedures to regulate dual use goods, which were considered in the European Parliament in September 2011 (P7_TA-PROV(2011)0406). Public consultations on the Green Paper on dual-use export controls[11] and widespread support for strengthening the existing dual-use regulatory regime suggest that Europe may yet achieve develop an effective ex ante regulation of dual-use goods.

As noted by the European Parliament in a recent resolution on April 18 2012, it is necessary not only to consider "increased transparency" (P7_TA-PROV(2012)0126) but also "accountability for EU-based companies, in order to improve the monitoring of the export of products and services aimed at blocking websites, mass surveillance, monitoring all Internet traffic and (mobile) communications, breaking into private conversations and transcribing them, filtering search results, and intimidating Internet users including human rights defenders" (P7_TA-PROV(2012)0126).

As Europe controls one of the largest markets for telecommunications and Internet technology in the world, it would seem obvious to exclude companies that have been proven by a court of law to export harmful technologies to repressive regimes from European public contracts. The policy model for such procedures can be taken from existing blacklisting mechanisms of the World Bank and the European Investment Bank. While such policy measures are less likely to be effective for companies trading in the 'worst of the worst' technologies, they may serve as a powerful mechanism to ensure compliance by manufactures of telecommunications hardware and Internet infrastructure, both inside and outside of Europe.

In contrast to companies that export the 'worst of the worst' technologies to repressive regimes, companies exporting dual use technologies have very different interests and are likely to be far more receptive to the right incentives. While far stronger regulatory measures will be necessary to gain greater control over the 'worst of the worst' industry, it can be hoped that with right incentives an intensive on-going multi-stakeholder dialogue and ultimately the threat of legislation, the 'dual use' group companies will have enough incentives to 'do the right thing.' As the primary markets for their goods are in Europe and North America, they are far more interested in access to these markets than harming human rights in secondary or tertiary markets in third countries.

3.4.2 Supporting the democratic control of intelligence services, law enforcement and military intelligence in third countries.

While many policy mechanisms within the debate on censorship and surveillance technologies have focused on the supply side of the equation, there has been as yet little debate on how to stem the demand for such technologies. The bodies purchasing such technologies are typically intelligence services, law enforcement or military intelligence in third countries. If such organisations gain access to such technologies, it should be strongly in the interests of the EU to ensure that basic democratic controls on such organisations exist.

Such democratic control is important as in many parts of the world, much of this repressive technological infrastructure is already in place and is likely to stay there for the foreseeable future. Even in countries in the MENA region that may slowly be becoming more democratic, the censorship and surveillance infrastructure is typically left in place and needs to be managed by institutions, which conform to basic democratic principles.

Best practices on how to organize the democratic control and supervision of intelligence services can be found in the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/14/46) and the *Study on Parliamentary Oversight of Security and Intelligence agencies in the European Union* (ATT27674) conducted

[11] For further information see: http://ec.europa.eu/trade/creating-opportunities/trade-topics/dual-use/

for the European Parliament's Civil Liberties, Justice and Home Affairs Committee. While the European Union has considerable experience in the area of security sector reform, there has been limited attention to establish oversight over the use of censorship and surveillance technologies in the programmes it is supporting. Both reports can be useful as a basis for policy initiatives in this area.

Supporting the spread and growth of democratic control of intelligence services, law enforcement or military intelligence in third countries has several advantages in the context of European debates on the harmful effects of communications technologies. First it may mitigate the harm caused by existing infrastructure that is currently in place. Second it may reduce the overall demand for additional infrastructure, systems or services, which could be harmful for human rights, particularly in regards to the 'worst of the worst' technologies. Third it is a policy mechanism that can be effective even for technologies sold by companies outside of Europe.

As the former CTO of a leading European telecommunications operator noted at a workshop on ICTs and human rights in the European Parliament recently, "the imagination of intelligence services is endless" (Fossier 2012). Engaging in a policy process, which ensures that the 'imagination' of such institutions is limited and accountable to the basic human rights principles, is likely to have substantial effects of the international trade in communications technology.

3.4.3 Make export loan guarantees, financial support and European funding for communications infrastructure conditional on human rights principles

Public sector organisations in Europe actively contribute to the creation and funding of repressive communications infrastructure outside of Europe. This has been best documented in the German Parliament, where the German government conceded to providing loan guarantees to companies exporting at best highly questionable technologies to regimes likely to abuse them (Krempl 2011; BT-DRS 17/8052). Another example is the creation of a video surveillance system in Saudi Arabian, where technical surveillance experts were recruited through the largest German Development Organisation GIZ (Lorscheid 2011).

More generally, as European public sector organisations are unaware or at times unwilling to acknowledge the potentially negative human rights impacts of the technologies whose export they are supporting, the European Union and its member states have considerable leverage in changing this status quo. By changing the basic conditions under which such financial support, export loan guarantees or other forms of public sector funding are available, European public sector organisations can directly contribute to ensuring that communications technologies are not misused to harm human rights. Indeed there is perhaps no other policy initiative in which European policy makers have such great leverage as the existing policy initiatives they are already paying for.

The complexity for this specific mid-term policy initiative lies in deciding whether communications infrastructure is likely to have a positive or negative impact on human rights and mainstreaming this decision making process across numerous decision making processes. In order to do so, European public sector organisations can in part learn from the private sector, which is faced by similar challenges and has an established set of tools at its disposal. Particularly the Human Rights Impact Assessment (HRIA) tools developed for the private sector by the Danish Institute of Human Rights would be valuable if they were employed in similar public sector initiatives.

When third country communications infrastructure is being publicly funded, the loans for the export of security technologies are being guaranteed or when third countries are being provided with publicly funded services to maintain or develop communications infrastructure, HRIA procedures can be highly effective. In nature they are quite similar to the *Human rights and democracy clauses*' called for in the European Parliament resolution of 18 April 2012 on the Annual Report on Human Rights in the World

(P7_TA-PROV(2012)0126). It also contributes to achieving the "rights based approach in development cooperation" (11855/12) outlined in the EU Action Plan on Human Rights and Democracy (11855/12).

What is missing however within the framework of the HRIA is a specific framework for dealing with communications infrastructure. While the Internet Rights and Principles Coalition has done excellent work in building a charter of human rights for the Internet, we still lack a multi-stakeholder document defining what kind of telecommunications and Internet infrastructure is desirable from a human rights perspective. The HRIA should ideally be based on a broader set of principles defining Human Rights Based Communications Infrastructure (HRBCI), the commitment to which however will need to be a long-term policy initiative.

3.5 Long Term European Policy Initiatives

Moving from medium-term to long-term policy initiatives, there are a number of goals, which can only be achieved in the long term. This is not to say that work upon them cannot begin immediately, but rather any reasonable or credible hope of achieving them can only exist in the long term. Consequently a long-term commitment to engaging in these policy initiatives is necessary to ensure that they can be achieved at all:

- Creating a multi-stakeholder process, which defines Human Rights Based Communications Infrastructure (HRBCI) and supports HRBCI in third countries.
- Establishing European initiatives to innovate for human rights and developing criteria for publicly funded European R&D projects to ensure that they promote human rights.
- Building a European body of knowledge on communications technologies and how they may enable or harm human rights.

3.5.1 Human Rights Based Communications Infrastructure (HRBCI)

What is the Internet we hope to create? Internet Architecture has increasingly shifted in the past decade towards allowing greater control - both public and private - of Internet users, network traffic and user data. Based on the experiences of the Arab Spring, the following template is a first draft of a set of conditions that could shift this balance back towards empowering end users:

a. Desirable Internet Infrastructure

- Lack of a technical 'kill-switch which could turn of the Internet at device or network level in accordance with international human rights standards.[12]
- Access to and support of strong encryption, authentication, and anonymity technology for Internet users.
- Permanent stable access to emergency services via all appropriate communications networks and channels.
- Multiple, independently operated international links and gateways per country.
- Multiple Internet exchange points (IXPs) per country.
- Community and mesh networks providing local decentralized communications.

[12] See the declaration *Joint Declaration on Freedom of Expression and the Internet* by the UN, OAS, OSCE and ACHPR for further details (La Rue, Mijatovic, Botero Marino and Tlakula 2011).

- Internet infrastructure owned and controlled by multiple non-state actors and at least in part by citizens themselves.
- Market-based non-state access to the 'last-mile' access to consumers.
- Redundant, competing communications networks employing diverse technological infrastructures.[13]

b. Desirable Communications Governance

- International human rights law as the constitutional basis for governance.
- Multistakeholder governance of key Internet resources.
- Non-state national domain name management.
- Multistakeholder IP address management.
- Liberalization of fixed line & mobile telephony markets.
- Liberalization of Internet provider market.
- Adherence to Network Neutrality principles.
- Full democratic oversight over any communications surveillance.
- Rule of law, due process guarantees and judicial oversight for any interventions on users' communication and sharing of any information gathered as a result of such interventions.
- Prevent technological and economic concentration in communications devices and infrastructure, to ensure an absence of single points of control.
- Support Internet users in properly assessing, managing, mitigating and making informed decisions on communications & ICT-related risks.
- Guaranteeing citizens access to communications networks without providing personally identifiable information.

Obviously such a document cannot be drafted by any one individual, but requires a multi-stakeholder process in which all relevant European actors are engaged. In this process the telecommunications sector guidelines, which are being developed by IHRB and Shift for the European Commission, the Charter of the Internet Rights and Principles Dynamic Coalition[14] and the short draft above may serve as a starting point for on-going discussions.

While the time frame for starting such a process is in the short term, it not clear whether the broad multi-stakeholder consultations required might not be a medium term policy initiative. In order for the whole initiative to be effective, however, there is a strong necessity to commit at a European level to supporting HRBCI in third countries in the long term. Only if the European Union and its member states are prepared to make such commitment, will stakeholders credibly engage with the EU and develop an inclusive document, which integrates the views of all relevant stakeholders.

[13] This is seen as one of the key foundations of a Human Rights Based Communications Infrastructure by Peter Franck, Chaos Computer Club (Franck 2012).

[14] Further information about the IRP Charter is available here: http://irpcharter.org/wpcharter/

In the context of the drafting of a HRBCI it will also be necessary to consider carefully whether European Standards – based on which much communications infrastructure is developed – need to be adapted in an appropriate manner to conform with European Foreign Policy aspirations expressed in HRBCI. Particularly the standards developed by the European Telecommunications Standards Institute (ETSI) on the *Handover interface for the lawful interception of telecommunications traffic* (TS 101 671 & ES 201 671) and on *Requirements of Law Enforcement Agencies* (TS 101 331) would need to be reconsidered.

3.5.2 Innovate for Human Rights & use HR-criteria for publicly funded European R&D

Europe is one of the most innovative areas for research and development in telecommunications and Internet technology in the world. Many of the current benefits to human rights enabled through communications technologies were developed by accident as a by-product of other initiatives. This in turn raises the question to what extent European innovation could produce technologies with the express intention of promoting human rights and empowering individuals.

Innovating for human rights could be a powerful tool for European policy to develop as part of on-going attempts to promote human rights on the Internet in third countries such as the European No Disconnect Strategy (COM(2011)200). However such initiatives must explicitly focus on empowering individuals regardless of where they are in the world and avoid focusing on specific regions or areas. Consequently innovation that focuses on developing tools and services, which empower users and protect their human rights are likely to be most effective. Some large European companies have already indicated their will to do precisely this and it can only be hoped that they will follow through on these commitments (Weidman 2012).

At the same time there is a necessity to ensure that existing European research projects disbursed by the European Science Foundation (ESF) or as part of FP7/FP8 framework programs consider basic human rights standards. In this context, the advisory service for FP7 research projects that is established by the FP7 project SURVEILLE seems to constitute one step in the right direction.[15] As noted above, the introduction of due diligence procedures are relevant not just for private sector but also for public sector actors although appropriate criteria are required.

A combination of innovation in the area of defending and protecting human rights in communications networks and guidelines for existing European research projects could have a considerable effect on European R&D output in the long term. While such initiatives are still at an early stage, they do suggest a long-term perspective in which human rights are designed into fundamental research and development processes within Europe.

3.5.3 Build a European body of knowledge on communications technologies and how they may enable or harm human rights.

In the entire field of human rights and the Internet there is a desperate need for a greater body of knowledge. This last long term initiative can be seen both as a commitment to evaluate existing European initiatives, to develop new initiatives based on a broader base of scientific and practical knowledge and to develop a better understanding of the phenomena based on which policy is being made.

This is not to say that the current European knowledge base is insufficient for policy making, but rather that European policy making in this area could be far more targeted and effective, given better knowledge about existing phenomena. This may refer to what the Vice-President of the European Commission, Neelie Kroes, referred to as 'Intelligence' as part of the No Disconnect Strategy, in her speech to the Dutch Freedom Online conference in Den Haag in December 2011.

While the No Disconnect Strategy represents an important first step in this regard, building a European body of knowledge on many of the issues above will require a long-term commitment to look at the

[15] For further information about the SURVEILLE ethical advisory service which is free for current and future technology developers receiving EU funding see: http://www.surveille.eu/index.php/advisory-service/. Other EU-funded research projects such as the ABC4EU FP7 project also intend to implement similar ethical review mechanisms.

questions raised by the strategy and many other related issues as well. There is a need to know both what is happening on the ground in many parts of the world and understand what this means in a wider scientific context.

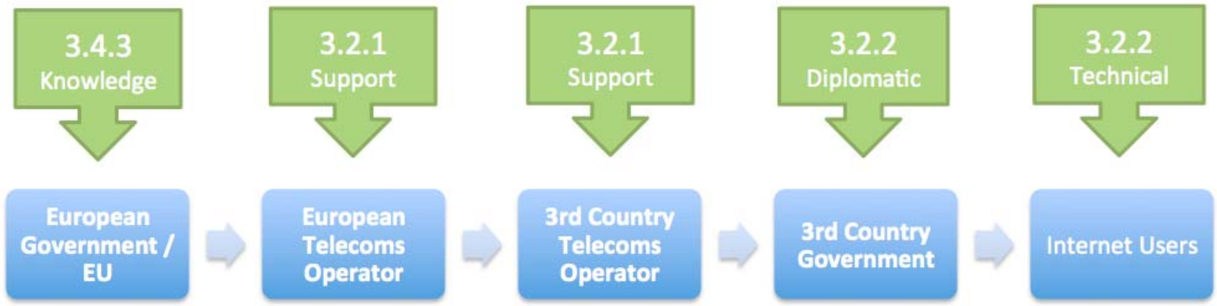
At best such a European body of knowledge could contribute to global debates on the effects of censorship and surveillance in societies across the world, could better understand the effects of circumvention technologies at an individual and societal level as well as analyse the impact of Internet Freedom both within Europe and beyond. Such knowledge cannot just be developed in European academia, but needs to be developed in collaboration with other international research institutions, civil society and businesses.

First attempts in this direction have already taken place in a Workshop between the European research program on the Future Internet (FIRE) and the No Disconnect Strategy in Brussels on 7 May 2012, will be taking place at several workshops at the Internet and Human Rights conference on 13-14 September in Berlin and at the Internet Governance Forum 2012 in Baku.[16]

Developing a European body of knowledge about these issues is essential in order to better 'see' and 'understand' the space in which policy is being developed. At the present time the policy space is so new and underdeveloped that additional research is essential. As many other organisations engaged in Internet Freedom initiatives have already discovered, developing effective policy and programming in the area of Internet Freedom is an extremely challenging task.[17]

3.6 Implementing European Policy Initiatives

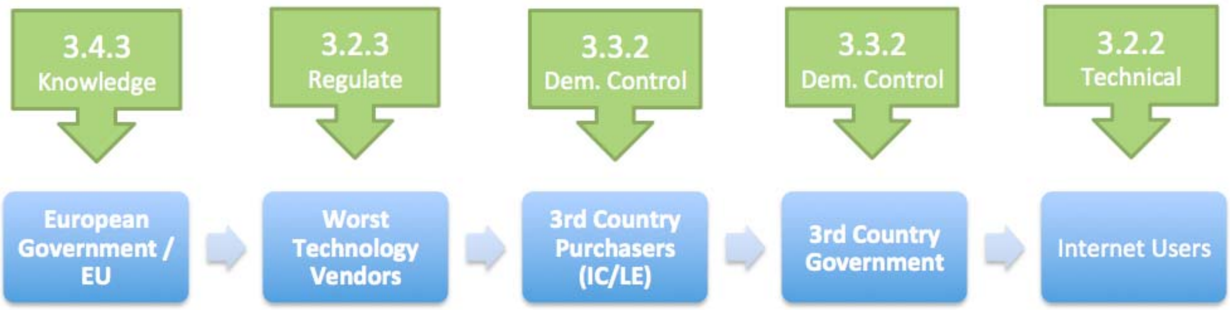
Having discussed the potential policy initiatives, this briefing paper will now attempt to embed these within the earlier mapping of European policy linkages and global supply chains. The previous mapping remains in blue while policy initiatives were added in green. In regards to telecommunications operators, several short and long term initiatives were proposed to make it more difficult to turn off the Internet in third countries:



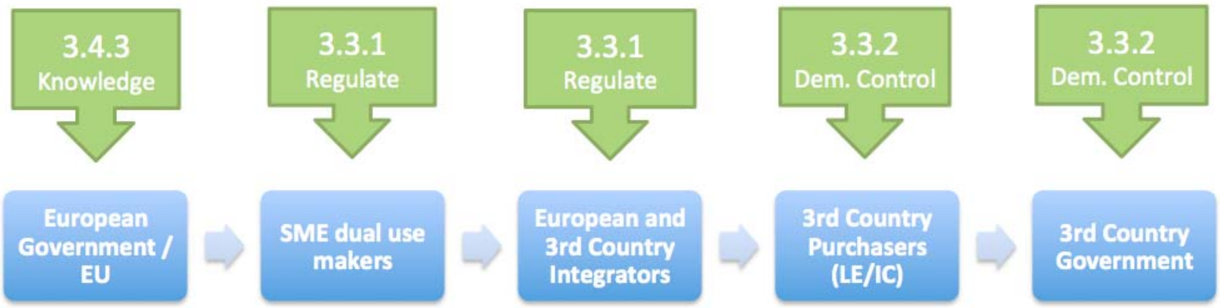
Then in regard to the 'worst of the worst' technologies, short, medium and long-term policy initiatives were proposed to tackle this phenomenon:

[16] For more information about these events please see http://cordis.europa.eu/fp7/ict/fire/events/evwsfirends_en.html http://www.internethumanrights.org and http://www.intgovforum.org.

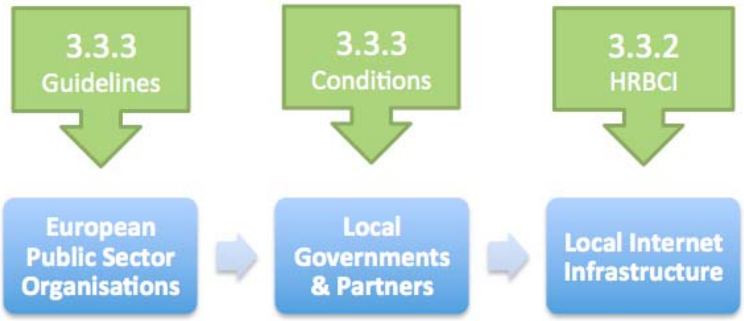
[17] For initial attempt at building comparative knowledge and understanding the challenges cross-nationally see: http://www.intgovforum.org/cms/component/content/article/116-workshop-proposals/1046-igf-2012-workshop-proposal--no-112-evaluating-internet-freedom-initiatives-what-works.



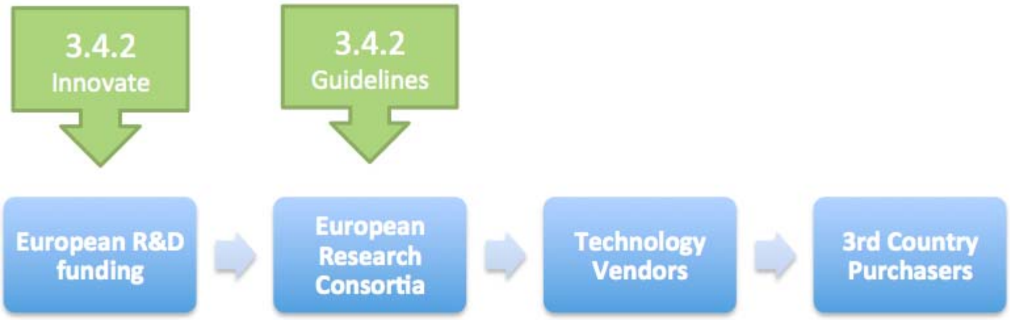
These policy initiatives are similar but distinct to those proposed for dual-use technologies, which require a different regulatory approach and different policy initiatives.



Equally it is important to remember that much of the communications infrastructure in third countries is partially funded by European donors. Consequently medium and long-term initiatives were proposed to ensure that European funding of communications infrastructure is consistent with European values.


3.3.3
Guidelines
3.3.3
Conditions
3.3.2
HRBCI
European Public Sector Organisations
Local Governments & Partners
Local Internet Infrastructure

Finally the role of publicly funded innovation and research spending is considered within a European context:



In all of these cases there are multiple policy options to influence the overall supply chain through European initiatives. While the process model is of course oversimplified, it may assist in understanding potential entry points for developing European policy in this area.

3.7 Conclusions

Europe has no strategic or foreign policy interest in supporting repressive regimes to harm the human rights of their citizens. Even if reasonable business interests of European companies are considered, it would be completely disproportionate to support small short-term profits despite massive harm of human rights enabled by the 'worst of the worst' technologies. Clearly there is a need to "make trade work in a way that helps human rights" (11855/12).

This briefing paper has made a number of recommendations for short, medium and long-term policy initiatives, which are likely to be effective. None of these strategies can be effective alone. Rather each policy initiative can be seen as a mitigation strategy, which may contribute to reducing harm. Particularly the medium and long-term strategies will require European policy makers to engage in a sustained multi-stakeholder dialogue with European businesses, civil society and governments on finding appropriate policy responses to the challenge of human rights on the Internet.

The Internet is a key enabler of human rights and allows individuals to seek, receive and impart information "unlike any other medium" (La Rue 2011, A/HRC/17/27). Supporting repressive regimes surveilling their citizens, controlling and censoring the Internet and restricting their fundamental rights isn't just bad human rights policy, it is bad foreign policy. Allowing such practices to continue will negatively affect the overall credibility of European Foreign policy towards third countries.

Notably it also has problematic consequences for European companies operating in third countries – who are often under the surveillance of these technologies. European companies are in danger of losing trade secrets and compromising internal customer data, with the help of other European companies who support third countries in surveilling and monitoring communications networks.

Europe has enormous political leverage to change this situation, as demonstrated in great detail earlier. There are very real choices to be made. This briefing paper has attempted to sketch out a variety of courses of action, any one of which could make a difference to the status quo. Of course, a wide range of measures targeting multiple points of political leverage would be most effective. Whether any of these policy options is actually implemented is a question of political will rather than a lack of policy options.

BIBLIOGRAPHY

Access. (2011). Vodafone: There's blood on your handsets. Retrieved from https://www.accessnow.org/page/s/vodafone-bloody-handsets

Chakchouk, M. (2011). Towards the Development of Broadband Internet in Tunisia: New Challenges, Opportunities and Perspectives. *3rd Arab Bloggers Meeting*. Tunis, Tunisia. Retrieved from www.slideshare.net/mchakchouk/ati-ab1103102011-9547841

Cowie, J. (2011). What Libya Learned from Egypt - Renesys Blog. *Renesys*. Retrieved from http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml

Dianotti, A., Squarcella, C., Alben, E., Claffy, K. C., Chiesa, M., Russo, M., & Pescap, A. (2011). Analysis of Country-wide Internet Outages Caused by Censorship. *Internet Measurement Conference (IMC)*. Berlin, Germany.

Deibert, R., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (2010). *Access controlled : the shaping of power, rights, and rule in cyberspace*. Cambridge Mass.: MIT Press. Retrieved from http://www.worldcat.org/title/access-controlled-the-shaping-of-power-rights-and-rule-in-cyberspace/oclc/457159952&referer=brief_results

Filastò, A. (2011). Blue Coat device logs indicate the levels of censorship in Syria. Retrieved from http://hellais.github.com/syria-censorship/

Fossier, M. (2012). Remarks by the Chief Corporate Social Responsibility Officer of the Orange Group. *Human rights and Communication Technologies: ICT - a double-edged Sword*. Brussels, Belgium. Retrieved from http://www.alde.eu/event-seminar/events-details/article/human-rights-and-communication-technologies-37916/

Franck, P. (2012). Peter Franck zu Freiheit und Sicherheit im Netz. eco e.V. Verband der deutschen Internetwirtschaft. Retrieved from http://www.eco.de/2012/news/peter-franck-zu-freiheit-und-sicherheit-im-netz.html

Human Rights Watch [HRW]. (2010). Egypt: Free Blogger Held Under Emergency Law. *Human Rights Watch*. Retrieved from http://www.hrw.org/print/news/2010/04/23/egypt-free-blogger-held-under-emergency-law

Human Rights Watch [HRW]. (2012a). World Report 2012: Libya. *Human Rights Watch*. Retrieved from http://www.hrw.org/world-report-2012/world-report-2012-libya

Human Rights Watch [HRW]. (2012b). *They Burned My Heart: War Crimes in Northern Idlib during Peace Plan Negotiations*.

Institute for Human Rights and Business [IHRB]. (2012). EU Sector Guidance. Retrieved from http://www.ihrb.org/project/eu-sector-guidance

Karr, T., & Le Coz, C. (2011). Corporations and the Arab Net Crackdown. *Foreign Policy in Focus*. Retrieved from http://www.fpif.org/articles/corporations_and_the_arab_net_crackdown

King, E. (2011). Big Brother Inc. *Privacy International*. Retrieved from https://www.privacyinternational.org/projects/big-brother-inc

Krempl, S. (2011). Bundesregierung hält an Export von Überwachungssoftware fest. *heise online*. Retrieved from http://www.heise.de/newsticker/meldung/Bundesregierung-haelt-an-Export-von-Ueberwachungssoftware-fest-1392507.html

La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the U.N. Human Rights Council [A/HRC/14/23]*. Geneva: United Nations.

La Rue, F., Mijatovic, D., Botero Marino, C., & Tlakula, F. P. (2011). *Joint Declaration on Freedom of Expression and the Internet*.

Lochbichler, B. (2011). Human Rights and Democracy: Waiting for the «silver thread» to become visible and credible. *Office for Promotion of Parliamentary*. Volume 3. December 2011. Brussels, Belgium.

Lorscheid, H. (2011). GIZ als Sponsor einer Rüstungsausstellung. *Telepolis. Heise*. Retrieved from http://heise-online.mobi/tp/artikel/35/35423/1.html

Mepham, D. (2012). Don't Kid Yourselves: Bahrain Hasn't Changed. *Human Rights Watch*. Retrieved from http://www.hrw.org/news/2012/04/18/don-t-kid-yourselves-bahrain-hasn-t-changed

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Nokia Siemens Networks [NSN]. (2012). Remarks by the Head of Government Relations, Finland of Nokia Siemens Networks Mr. Kristo Lehtonen. Human rights and Communication Technologies: ICT - a double-edged Sword. Brussels, Belgium. Retrieved from http://www.alde.eu/event-seminar/events-details/article/human-rights-and-communication-technologies-37916/

Noman, H. (2009). Middle East and North Africa. *OpenNet Initiative*. Retrieved from http://opennet.net/research/regions/mena

Noman, H., & York, J. C. (2011). *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011*.

Noman, H., & Zarwan, E. (2007). Internet Filtering in the Middle East and North Africa. *OpenNet Initiative*. Retrieved from http://opennet.net/studies/mena2007.

Organisation for Economic Co-operation and Development [OECD]. (2008). Accra Agenda for Action. Paris: OECD.

Ragan, S. (2010). Tunisian government harvesting usernames and passwords. Retrieved from http://www.thetechherald.com/article.php/201101/6651/Tunisian-government-harvesting-usernames-and-passwords

Reporters Without Borders [RSF]. (2005). The 15 enemies of the Internet and other countries to watch - Reporters Without Borders. *Reporters Without Borders*. Retrieved from http://en.rsf.org/the-15-enemies-of-the-internet-and-17-11-2005,15613.html

Reporters Without Borders [RSF]. (2012). Egypt - Reporters Without Borders. *Reporters Without Borders*. Retrieved from http://en.rsf.org/egypt-egypt-12-03-2012,42049.html

Schaake, M. (2011). Letter to HR/VP C. Ashton about internet disconnection in Egypt. Brussels, Belgium: European Parliament. Retrieved from http://www.marietjeschaake.eu/2011/01/letter-to-hrvp-c-ashton-about-internet-disconnection-in-egypt/

Silver, V. (2011). Post-Revolt Tunisia Can Alter E-Mail With `Big Brother' Software - Bloomberg. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html

Silver, V., & Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Sonne, P., & Coker, M. (2011). Foreign Firms Helped Gadhafi Spy on Libyans. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

Sonne, P., & Gauthier-Villars, D. (2012). Tech Firm Amesys Faces French Judicial Probe -WSJ.com. Retrieved from http://online.wsj.com/article/SB10001424052702304791704577420392081640000.html

Sutton, M. (2012). Syria Arrests Razan Ghazzawi and Eleven Other Activists in Renewed Crackdown of Online Dissent | Electronic Frontier Foundation. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2012/02/twelve-syrian-activists-arrested-amid-renewed-crackdown

Terrab, M., Serot, A., & Rossotto, C. (2004). *Meeting the Competitiveness Challenge in the Middle East and North Africa*.

Varoudakis, A., & Rossotto, C. M. (2004). Regulatory reform and performance in telecommunications: unrealized potential in the MENA countries. *Telecommunications policy*. *28*(1).

Wagner, B. (2012a). Push-Button-Autocracy in Tunisia: Analysing the role of Internet Infrastructure, Institutions and International Markets in Creating a Tunisian Censorship Regime. *Telecommunications Policy*, *36*(6).

Wagner, B. (2012b). *Exporting Censorship and Surveillance Technology*. Den Haag, The Netherlands. Retrieved from http://www.hivos.nl/eng/Hivos-Knowledge-Programme/Themes/Digital-Natives-with-a-Cause/Publications/Exporting-Censorship-and-Surveillance-Technology

Weidman, E. (2012). Internet freedom in the Networked Society - The Networked Society Blog. *The Networked Society Blog. Ericsson.* Retrieved from http://www.ericsson.com/thinkingahead/the-networked-society-blog/2012/04/19/internet-freedom/

York, J. (2012). The Arab Digital Vanguard: How a Decade of Blogging Contributed to a Year of Revolution. *Georgetown Journal of International Affairs*, (Winter/Spring 2012).

ANNEX 1: An overview of Demand: 45 Governmental Organisations from 15 countries in the MENA Region that Attended Trade Shows for Surveillance Technologies, derived from the *Surveillance Who's Who* by Privacy International[18]

- Embassy of Morocco
- Government of Morocco
- Morocco Ministry of Interior
- Morocco National Defense (CSDN)
- Royaume Du Maroc
- Egypt Ministry of Interior
- Egypt National Security Agency
- Egypt Telecommunications Regulatory
- Embassy of Egypt
- Government of Egypt
- Oman Ministry of Defence
- Oman Ministry of Interior
- Oman Royal Army
- Oman Telecommunications Regulatory
- Sultan Kabous Royal Court
- Bahrain Ministry of Interior
- Bahrain National Security Agency
- Bahrain Public Prosecution
- Bahrain Telecoms Regulatory Authority
- Jordan Army Force
- Jordan Electronic Warfare
- Jordan Telecommunications Regulatory
- Libya IT Crime Prevention
- Libya NSA
- Libya State Security
- Palestinian Authority President's Office
- Lebanon Ministry of Telecommunication
- Tunis Ministry of Interior
- Tunis Telecom Authority
- Kuwait Defense and Government
- Kuwait Ministry of Communications
- Kuwait Ministry of Interior
- Yemen MACSOL
- Yemen Ministry of Interior
- Yemen National Security Agency
- Private Office of Khalid Masnad (Qatar)
- Qatar Law Enforcement Agency
- Qatar Ministry of Interior

[18] This list of MENA countries is directly taken from the global list in the *Surveillance Who's Who* by Privacy International. A full global list can be found here: http://bigbrotherinc.org/v1/

- Iraq Office
- Iraqi Prime Minister
- Libya IT Crime Prevention
- Libya NSA
- Libya State Security
- Algeria Telecom Regulatory
- Algerian Ministere de la Poste

ANNEX 2: ADDITIONAL DOCUMENTS AND RESOURCES

Want to find out more? This section is a starting point for additional resources and information on issues related to this document. It is designed to allow easy follow-up research as well as providing the interested reader with further reading material.

The Censorship and Surveillance Technologies & Human Rights

- Wired for Repression: http://www.bloomberg.com/data-visualization/wired-for-repression/
- Bugged Planet: http://buggedplanet.info/
- Big Brother Inc: https://www.privacyinternational.org/projects/big-brother-inc
- OWNI Spyfiles: http://www.spyfiles.org/
- Censorship Inc: http://topics.wsj.com/subject/C/censorship-inc/6743
- Wikileaks The Spyfiles: http://wikileaks.org/the-spyfiles.html

Diplomatic Initiatives Promoting Human Rights on the Internet

- Remarks on Internet Freedom, Hillary Clinton, Washington DC: http://www.state.gov/secretary/rm/2010/01/135519.htm
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the U.N. Human Rights Council: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Freedom Online, The Hague: http://www.minbuza.nl/en/ministry/conference-on-internet-freedom
- Stockholm Internet Forum: http://www.stockholminternetforum.se/
- Berlin Conference on Internet and Human Rights: http://www.internethumanrights.org

EUROPEAN PARLIAMENT

BB-32-12-238-EN-N

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

Foreign Affairs

Human Rights

Security and Defence

Development

International Trade

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

ISBN 978-92-823-3782-0

9 789282 337820

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-3782-0
doi: 10.2861/9556

Publications Office