BEN WAGNER

EXPORTING CENSORSHIP AND SURVEILLANCE TECHNOLOGY

Hivos
people unlimited

Colophon

January 2012

Humanist Institute for Co-operation with Developing Countries (Hivos)
P.O. Box 85565 | 2508 CG The Hague | The Netherlands
www.hivos.net

Design: Tangerine – Design & communicatie advies, Rotterdam, The Netherlands

ISSN 2212-618X

© Hivos
This work is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 Netherlands License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/3.0/nl/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

EXPORTING CENSORSHIP AND SURVEILLANCE TECHNOLOGY

Table of Contents

1) Introduction 7

2) Exporting Censorship and Surveillance Technology 7

3) Additional cases of trade in censorship and surveillance technology in the MENA region 11

4) The Human Rights Impact: Case Study Tunisia 12

5) Corporate Governance 12

6) Public and Foreign Policy 13

7) Conclusions 14

8) Bibliography 15

Exporting Censorship and Surveillance Technology
By Ben Wagner

1) Introduction

> "[G]overnments have never met a voice or public sphere they didn't want to control at some point or another. They want to control what gets printed in newspapers, who gets into universities, what companies get oil contracts, what churches and NGOs get registered, where citizens can gather, so why not the Internet?" (Clinton 2011)

While it has become common knowledge that surveillance and censorship technologies are frequently exported across the world, the extent to which this is taking place has only become apparent in recent years. Public reports on censorship and surveillance technologies created by Nokia Siemens Networks being used in Iran, by Ericsson in Belarus, by SmartFilter in Tunisia and by Narus in Egypt are all suggesting substantial human rights implications. In response to these concerns the Global Network Initiative in the U.S. has initiated a self-regulatory framework for Internet companies to respond to these concerns. In Europe the European Parliament, the United States Congress and several European governments have expressed a desire to regulate these technologies more extensively.

This paper will discuss what we know about the export of Internet technology, before looking at the specific cases of exports of censorship and surveillance technology to Tunisia, Syria, Egypt and Libya. After briefly mentioning additional cases, which have received widespread public attention in 2011, it will then focus on at the specific human rights impact that censorship and surveillance technologies had in Tunisia. Subsequently, the global corporate governance responses will be listed before additional public policy measures are discussed. In conclusion, the paper will look at potential future directions in the trade in censorship and surveillance technologies, before providing key recommendations to the different stakeholders involved.

As with any other form of technology, the hardware and software at the basis of censorship technology is essentially value neutral. Hence 'censorship technology' and 'surveillance technology' are relational concepts, which exist in certain contexts but cannot be generalised to all possible uses of this technology. The legal term to typically describe this kind of technology is 'dual use' which suggests both military and non-military uses of certain types of technology. At the same time it is important to note that typical censorship and surveillance technologies are sold as systems and are not typically used for multiple overlapping purposes. Although the base hardware is theoretically capable of performing multiple diverse tasks, the systems themselves are typically built and maintained for one specific purpose: limiting individual human rights. Consequently some of the technologies suggested to be 'dual use' are effectively 'single use' technologies. These systems are so fundamentally designed to invade basic human rights that it becomes difficult to ascertain 'legitimate' or 'lawful' purposes, within which such technologies might be used.

2) Exporting Censorship and Surveillance Technology

a) Tunisia

Following the Jasmine revolution in Tunisia, there has been much debate both at a national and international level about the Internet censorship infrastructure in the country. In order to establish such a system the Tunisian government received extensive support from international corporations to build and maintain its censorship infrastructure. One important element of the system is a classification database of sites used to identify sites, which will be censored. In Tunisia, this has historically been executed by SmartFilter, which is also used for censorship by other states in the Middle East and North Africa (OpenNet Initiative 2009). Smartfilter is a product of Secure Computing, a company that was recently acquired as part of the McAfee by Intel (Noman and York 2011).

However to enable filtering in Tunisia a second layer of technology infrastructure is required to actively implement this filtering software across Tunisia. There are strong indications that since 2007 Tunisia have been using deep packet inspection (DPI) to censor their national Internet, based on the Smartfilter website categorisation database (Wagner 2008). However deep packet inspection technology is not developed in Tunisia and there is not a single Tunisian vendor or integrator capable of providing countrywide DPI solutions to the Tunisian state.

Like other countries employing DPI and filtering solutions within their censorship and control infrastructures in the Middle East and North Africa, it seems evident that Tunisia uses DPI developed and sold by European and North American vendors. In Tunisia this filtering technology was provided by Blue Coat Systems, NetApp and Ultimaco (Silver 2011a). There are also reports that suggest that Detica may have sold surveillance technology to Tunisia (HL Deb, 21 November 2011, c210W). This external sourcing of DPI contributes to ongoing support costs for the filtering equipment, which extends beyond the initial deployment of filtering technology itself. Figures from the Agence Tunisienne d'Internet suggest that these costs have amounted to over 1 million Tunisian dinars per year (at the time around 570.000 Euros) since 2007, rising to around 3.6 million Tunisian dinars (at the time around 2 million Euros) in 2010 (Chakchouk 2011).

Furthermore there are strong suggestions that Tunisia employs multiple separate surveillance infrastructure. The companies involved in creating and maintaining Tunisian surveillance infrastructure include Nokia Siemens Networks, ETI (a subsidiary of BAE Systems), Blue Coat Systems, NetApp, Ultimaco and Trovicor (Silver 2011a). The seeming involvement of multiple different European and U.S. companies is not untypical, although Tunisia does represent one of the countries where the censorship and surveillance regime was particularly broad. It should come as little surprise in this context that Tunisia was used as a country wide 'test bed' for various kinds of censorship and surveillance technology. Consequently the Tunisian government was given a substantial discount so that international corporations could 'try out' their technology on a national scale in Tunisia (Chakchouk 2011). In many cases, these technologies were later deployed elsewhere in the MENA region.

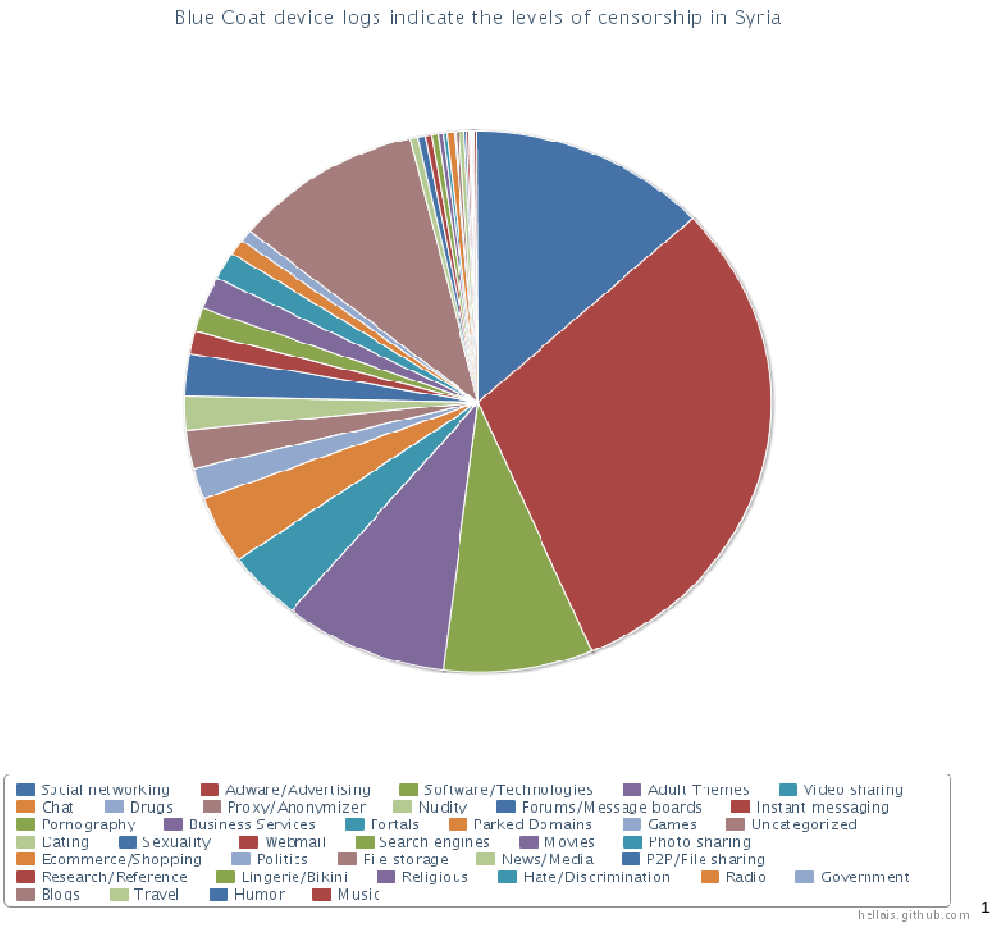
Closely linked to the purchase of internationally sourced censorship and surveillance technology is the long-standing support of the Tunisian censorship and control regime by European technical consultants - particularly from France and Germany. Their role has mainly been to provide important maintenance and technical support services for the Tunisian censorship regime. The French Internet service provider Wanadoo is one of the most important providers of technical support to the Tunisian state in this regard (Krempl 2008). Due to relatively unrestricted access to international technology markets, large Tunisian companies were also able to purchase DPI-solutions and employ them to monitor their employees and customers. Consequently there are numerous DPI solutions employed in Tunisia from a variety of different European and North American vendors, many of which are associated with considerable human rights concerns.

b) Syria

For a long time very little was known about the extent of censorship and surveillance technology in Syria. While it has been common knowledge that such technology was in use, it was very hard to ascertain which kinds of solutions were being employed, let alone who the vendors of these solutions were. During the widespread public protests and uprising in Syria, however, this changed dramatically. This is likely due to the increased public attention during the uprising, the violent governmental response and the pariah status of Syria in the international community. Most importantly however both in Syria, Egypt and elsewhere in the MENA region, the uprising period seems to have been interpreted as a particularly effective sales period by the vendors of censorship and surveillance technologies. As a result the existing censorship and surveillance technologies were supplemented with additional layers of technology. These are specifically designed to give the government greater ability to "crackdown on protests" (Elgin and Silver 2011) and provide additional surveillance capacity to the Syrian government.

A conglomerate of European and U.S. companies were involved in the project. These were Area SpA from Italy, Ultimaco from Germany, Hewlet-Packard and NetApp from the United Stated as well as Qosmos from France (Elgin and Silver 2011). However these installations only represented additional surveillance technology to what was already installed in the country. The Syrian government was clearly using surveillance technology produced by Blue Coat Systems, which seems to have made it's way into the country via Iraq (Waleed 2011). Although it also seems reasonable to ask why such products were being sold to Iraq, their eventual use in Syria is clearly highly problematic from a Human Rights perspective. There is also an ongoing debate on whether the Iraqi government played an active, passive or completely non-existent role in the devices reaching their destination in Syria (Waleed 2011).

It is equally problematic that the devices were not sufficiently secured from external access by their operators. While this did allow activist group Telecomix to post logs they generated online, it also allowed access from other actors and groups. One of the inherent problems with the addition of restrictive technologies to communications networks is that they provide additional vectors for attack and misuse by third parties. Admittedly this may have actually been helpful this context to allow whistleblowers to raise awareness about the existence and use of such technologies. Nevertheless the substantial risk to individuals employing these communications networks should not be underestimated. Examining the information that was published by Telecomix, Internet users have begun chronicling the various uses of the Internet that were captured by the technology (Filastò 2011):



[1]

The chart clearly shows the power of surveillance technology to delve into almost all aspects of personal communication online. From social networking and chat, to business services, photo sharing and of course pornography, all aspects of individuals private lives are open for view. Of significant concern are also logs showing traffic which users believed was protected through encryption. Here surveillance technology takes

[1] Filastò, Arturo. 2011. "Blue Coat device logs indicate the levels of censorship in Syria." Retrieved December 17, 2011 (http://hellais.github.com/syria-censorship/).

away the presumed anonymity of users, even if they have taken specific precautions to ensure that both their identity and the content of their communications cannot be read.

While the Syrian government showcases some of the worst censorship and surveillance technology, it is equally symptomatic for many other states in the MENA region. Existing censorship and surveillance infrastructures are employed broadly and extensively expanded in times of crisis and popular unrest. In both contexts international technology markets, which provide the underlying technology with almost no regulation, are key to this process.

c) Egypt

Egypt is another particularly interesting case within the MENA region. The centrality of the country and the importance of its media industry to the wider region have long made Egypt itself one of the key actors within the region (Abdulla 2007). The role of Egypt in the MENA region is also notable because it seems to suggest that it was one of the few countries in the region that did not employ a broad Internet filtering infrastructure (OpenNet Initiative 2009). This stance however is deceptively liberal, as a closer look at d other measures of limiting press freedoms quickly paints a different picture. This picture is one of widespread Internet surveillance, of intimidation and forced disappearance of bloggers and Internet activists and a culture of fear that spreads across the Internet in Egypt. These measures were consistent with the overall perception of the Egyptian 'Mukhabarat State' in which political speech was highly restricted (Hudson 1991).

Parts of the overall surveillance infrastructure in Egypt were provided by Narus, an American company based in California which is a subsidiary of Boeing and sold surveillance technology to Telecom Egypt, the largest and oldest telecommunications provider in Egypt (Karr 2011). The relationship between Telecom Egypt and Narus seems to have been mediated by a local Egyptian consulting firm, Giza Systems. Giza was responsible for the installation of Narus technology on Telecom Egypt's networks and had close links to other providers of deep packet inspection technology across the world. They provided Narus and other censorship and surveillance technology to the Egyptian government and various other countries across the Middle East.

Similar to Tunisia and Syria, Egypt took aggressive steps to increase its surveillance regime during public protests in 2010/2011. These began with increased surveillance and arrests of key Internet activists and bloggers and culminated in disconnecting the entire Internet in Egypt for several days. During this period there are well-documented international reports that link the former Egyptian government to `Trojan Horse` surveillance technology provided by Gamma International (Saoub 2011), a British-based company that operates mainly in Germany. This clearly represents a technological escalation during a popular uprising similar to the Area contract in Syria. Additional technology is delivered specifically for the express purpose of providing the state with additional surveillance technology during a period of widespread public uprising. This technology can only be traded in these specific contexts and can only lead to the assumption that it will be used to violate human rights. Offering this technology to Egyptian State Security in this context goes far beyond corporate disregard for human rights implications. It suggests clear intent by the company involved that their product would be used for human rights violations.

d) Libya

After the protests in Egypt and Tunisia, Libya was another country where popular uprising and eventually revolution took place during the Arab spring. The uprising in Libya, however, did not come unexpected and the regime had already taken various measures to be able to suppress protests. This included an extensive surveillance infrastructure purchased from European and North American vendors, as well as one vendor from China. The Egyptian company Giza Systems also features heavily in the Libyan case, as there have been credible reports linking Narus technology in Libya to Giza Systems (Karr and Le Coz 2011). Nonetheless it seems that there were many other companies involved in the provision of surveillance technology to Libya: Amesys, ZTE Corp. and VASTech (Sonne and Coker 2011). Amesys is a business unit within the French technology company Bull SA, which seems to have been responsible for building a

telecommunications-monitoring centre. ZTE Corp. from China seems to have provided additional technical infrastructure while VASTech SA Pty Ltd is reported to have contributed technology used to record international phone calls (Sonne and Coker 2011).

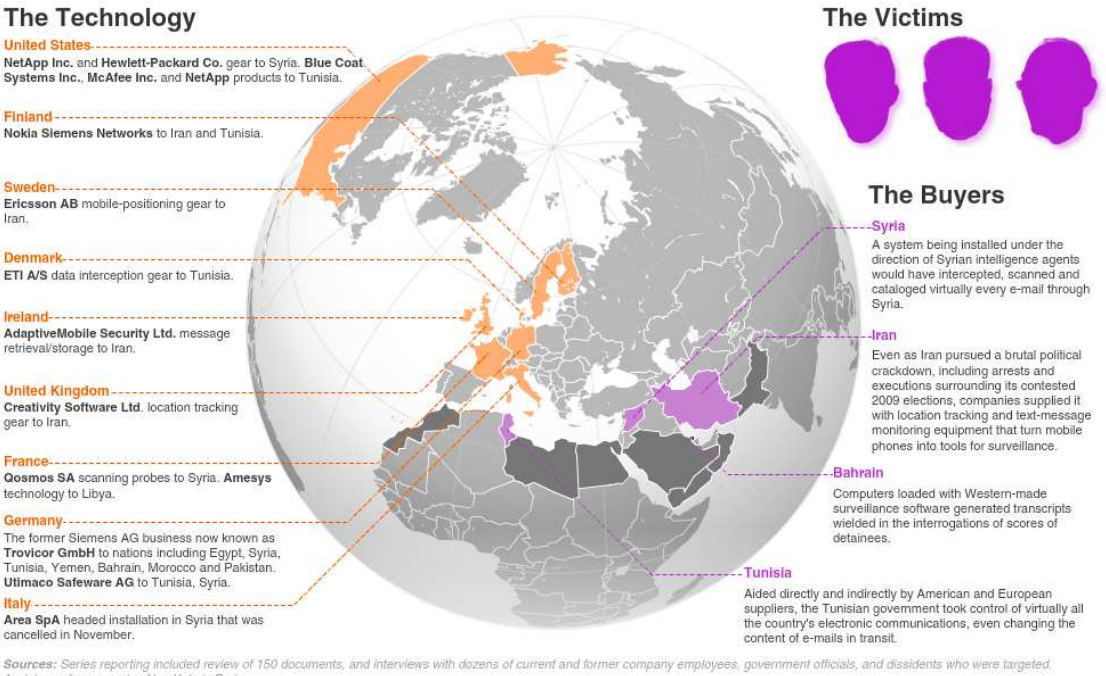
Like Egypt, Libya also decided to cut its citizens off from the public Internet for an extended period when mass protests broke out. However in the Libyan case the government seems to have learnt from the Egyptian experience and massively slowed down the Internet rather than completely blocking it (Cowie 2011). This development suggests that there is an ongoing learning process between different authoritarian regimes. Each 'turning off' of the Internet became slightly more advanced as technological developments progressed, ensuring greater effectiveness of these suppression techniques.

3) Additional cases of trade in censorship and surveillance technology in the MENA region

Beyond the mentioned cases there have been extensive reports in 2010 & 2011 on the export of censorship and surveillance technologies. Such has been the extent of these reports that they create the impression that in every authoritarian state where mass public protests or revolutions take place, European and North American censorship and surveillance technology will eventually be found. To provide a few short examples:

- In Iran, Nokia Siemens Networks is accused of have exported mobile phone surveillance technology to the country (Lake 2009).
- In Bahrain, Trovicor and Nokia Siemens Networks provided surveillance technology, which was used to identify activists who were later tortured (Silver and Elgin 2011).
- The McAfee Smartfilter database of sites is used censor the Internet in Saudi Arabia, UAE, Kuwait, Bahrain, Oman and Tunisia (Noman and York 2011).
- Yemen, Oman, Saudi Arabia, and Morocco are reported to be using surveillance technology provided by Trovicor (Elgin, Silver and Zschiegner 2011).

The following map also provides an overview of much of the surveillance technology being exported to the MENA region:



[2] Elgin, Ben, Vernon Silver, and Hermann Zschiegner. 2011. "Wired For Repression." Bloomberg. Retrieved December 20, 2011 (http://www.bloomberg.com/data-visualization/wired-for-repression/).

This list is by no means exhaustive. Rather it is likely to represent only the tip of the iceberg and that each revolution or public uprising in an authoritarian state will bring forth new cases of censorship and surveillance technology from European and North American companies. Additional resources can be found on the following websites:

- Bugged Planet: http://buggedplanet.info/
- Privacy International - Big Brother Inc: http://bigbrotherinc.org/
- OWNI Spyfiles: http://www.spyfiles.org/
- Wired for Repression: http://topics.bloomberg.com/wired-for-repression/
- Censorship Inc: http://topics.wsj.com/subject/C/censorship-inc/6743
- Wikileaks The Spyfiles: http://wikileaks.org/the-spyfiles.html

4) The Human Rights Impact: Case Study Tunisia

The extensive architecture of Internet censorship in Tunisia allows for specific targeting of individual activists, activist groups and specific types of content. This can be both in the form of targeting certain Internet sites or keywords, restriction of specific individuals' ability to access the Internet, attacking specific sites and any mixture of the above. As noted by Eric Goldstein from Human Rights Watch:

> "Ben Ali could have simply shut down local human-rights groups and jailed their founders. But that would have run counter to the image he wished to project. So he let these groups exist-barely-while employing hundreds of goons to harass their members, block their meetings, and scare away the victims of government abuse who sought their help" (Goldstein 2011).

The Internet control regime is an important component of an overall strategy to project a positive image of Tunisia to the outside world. At the same time his close ties to Western states ensured he had unfettered access to transnational technology markets, where international corporations compete to provide some of the most advanced censorship technologies to authoritarian states.

This censorship infrastructure also played an important role during the Jasmine revolution in Tunisia (Wagner 2011). After the beginning of widespread popular protests in Tunisia in December 2010, existing Internet censorship and control were increased and the "head of the Agence Tunisienne d'Internet (ATI) [confirmed that] the number of websites blocked by the authorities [had] doubled in just a few weeks (Reporters without Borders 2011). At the same time, the government orchestrated "cyber attacks" on Internet activists, journalists and bloggers, breaking into the Facebook accounts and Facebook groups of activists and defacing or deleting their websites and blogs (Ragan 2011).

Closely linked to this were targeted arrests of bloggers, journalists and Internet activists on January 7th, 2011, a "string of arrests that come in the midst of what is being described as a nationwide uprising" (Ryan 2011). The specific targeting of bloggers, journalists and Internet activists suggests that censorship technology is part of a wider system of repression and control (Wagner 2011). It serves not only to stifle expression and gain control over dissemination of information about protests, but also to chill potential speech and expand the shadow of hierarchy of state power far beyond existing expression boundaries.

5) Corporate Governance

Given the substantial Human Rights concerns associated with censorship and surveillance technologies, it seems reasonable to expect some corporate response to these concerns. One possible response could be extending existing corporate auditing processes to also consider their human rights impact. Consequently existing due diligence processes would also take into account the potential impact on Freedom of Expression of the sale of these technologies, for example by use of Human Rights Impact Assessments (HRIAs). Such a development would significantly change the supply-side economics of censorship technologies.

To a certain extent due diligence on freedom of expression and human rights is clearly taking place and some companies are refusing to sell censorship and surveillance technologies to heavily authoritarian states. Many of the exporting companies have existing ethical standards on which they based their export decisions. At the same time it should be noted that decisions based on these standards are often heavily disputed within companies and it is not uncommon to hear of internal regulations being overturned if the terms are favourable enough. Moreover this still leaves a substantial group of companies who are prepared to do business with almost any country in the world. They care little for export regulation and are prepared to go to almost any means to evade existing restrictions.

Another avenue that has been explored is the joint self-regulatory framework espoused by the Global Network Initiative (GNI). Notably the current GNI corporate participants, Google, Microsoft and Yahoo predominantly provide software or online services. Without doubt there have been many attempts to bring them on board, but not a single hardware vendor could be persuaded to become a GNI participant, although there have been numerous discussion with these corporations. Admittedly, two additional companies have been persuaded to join GNI with both Evoca and Websense joining in late 2011. However to this day it remains difficult to assess the progress on actual business practices has been made by GNI members.

This raises the question whether human rights concerns associated with censorship and surveillance technologies can be resolved within self-regulatory frameworks or whether other forms of governance could be more appropriate. The Global Network Initiative was a direct product of U.S. government pressure on technology companies to self-regulate, following reports about the complicity of U.S. corporations with human rights violations in China. In a statement to an international conference of foreign ministers on Internet freedom in Den Haag, the vice president of the European Commission Neelie Kroes called on companies to make similar commitments:

> "Self regulation could help here. The industry should come up with concrete solutions. The Global Network Initiative is one possible model, but I don't want to be prescriptive at this stage. But I do want to see some kind of action. For our part, we are ready to support that process with expertise and operational support" (Kroes 2011).

This suggests that pressure may be increasing on European countries to come up with solutions sooner rather than later. At the same time, it should be noted that self-regulation both in Europe and the U.S. is a direct consequence of pressure exerted by governments and negative public attention. Moreover there are many contexts in which relying solely on self-regulatory solutions is likely to be insufficient. Additional regulatory mechanisms are likely to be required to create meaningful changes to the status quo.

6) Public and Foreign Policy

The European Parliament has probably been the most active proponent of a public policy solution to the export of censorship and surveillance technologies, with several parliamentary resolutions highly critical of the export of surveillance technologies to autocratic states. These have been followed-up by numerous written requests by European Parliamentarians to the Commission, most notably by Marietje Schaake (ALDE) a Dutch MEP who has been lobbying heavily for change on this issue. The European Commission has been relatively slow to act and has provided only limited responses to the many questions MEPs have posed (EP: E-8813/2010). However the European Commission has begun to introduce additional limitations on surveillance technologies in states such as Syria (EC: PR 469 Nr: 17895/11).

Another important initiative was the bill introduced by Austrian MEP Jörg Leichtfried, which specifically focuses on providing greater transparency on exports of surveillance technologies from the EU. It also prevents blanket export exemptions of dual-use goods which can be used to harm "human rights, democratic principles or freedom of speech" (EP: P7_TA-PROV(2011)0406). It also includes links restrictions on dual use goods to future sanctions regimes imposed by the OSCE, the U.N. Security Council or the EU. While a significant step forward, Leichtfried believes that more would have been possible and

what he had hoped to achieve was an “advance notification system” (Leichtfried 2011). Such a system could indeed be very effective at preventing additional exports of technologies by publishing details of the export before it has actually taken place. Another concern are the various national export legislations which are still applied in many cases relating to dual use and are likely to allow a greater number of exports than is currently the case.

At a national level, the Dutch Ministry of Foreign Affairs (MFA) has been an active participant in the debate on the export of censorship and surveillance technologies (de Vreij 2011). The Dutch MFA has repeatedly suggested that he wishes to go beyond current conceptions of Internet Freedom - which as espoused in the U.S. prefer self-regulatory solutions - and develop public policy solutions to promote Internet Freedom (Rosenthal 2011). The Swedish MFA, while one of the countries pushing very strongly for Human Rights on the Internet (Bildt 2011) has been less enthusiastic about the issue of export controls. What has been described as the “Ericsson factor” (Guibourg 2011) seems to have been an important limiting factor for Swedish support for greater regulatory control of censorship and surveillance technologies. Similarly the German MFA have shown some appetite for pursuing an Internet freedom agenda in foreign policy (Westerwelle 2011) however they have shied away from pursuing restrictive policies on dual use products (DER SPIEGEL 2011). While the German government continues to guarantee the loans of German corporations exporting surveillance technologies (Krempl 2011; BT-DRS 17/8052) it is hard to see how they intend to pursue an Internet freedom as part of wider foreign policy.

In the United States there is still strong resistance to any form of ‘hard’ regulation that goes beyond self-regulatory solutions such as those developed by the Global Network Initiative. However an important report by the bipartisan think-tank ‘Center for New American Security’ recently suggested reforming export regulations precisely to this effect (Fontaine and Rogers 2011). Despite strong resistance to hard regulation in this area, the Global Online Freedom Act is again being proposed in the U.S. congress (Elgin 2011). It was first proposed in 2006 by Congressman Chris Smith (Republican, New Jersey) and was re-introduced in 2009 and 2011 (H.R. 4780 [109th]; H.R. 2271 [111th]; H.R. 3605[112th]). While there is clearly room to improve the bill itself, it does represent another important legislative step on the way to any overall regulatory regime to govern the trade in censorship and surveillance technologies.

Separately the U.S. Government Accountability Office (GAO) was asked to produce a report (GAO-11-706R) identifying U.S. companies which had exported censorship and surveillance technology to Iran. Given the limited resources and investigatory powers at their disposal, they found it difficult to specify which U.S. companies could be exporting surveillance and censorship technologies to Iran. Notably Internet Freedom was included in the U.S. International Strategy for Cyberspace in May 2011, although here it explicitly refrains from mentioning export controls or similar restriction on the trade in technologies. (National Security Council (U.S.), & United States. Executive Office of the President. 2011).

Still the Joint Action for Free Expression on the Internet in the Hague on 9 December 2011 does provide room for optimism, with Austria, Canada, the Czech Republic, France, Estonia, Ghana, the Republic of Ireland, Kenya, Mexico, Mongolia, the Netherlands, the United Kingdom, the United States, and Sweden endorsing a joint statement and dedicating themselves to:

> “Engaging together as members of this coalition with information and communication technology businesses from across the globe on their responsibility to respect human rights and fundamental freedoms online” (Final Declaration 2011).

Whether the participating states will follow through on this commitment remains to be seen. While it is possible that other states will join the declaration at a later stage, it is difficult to determine at this stage what the overall effect on internet foreign policy will be.

7) Conclusions

> “We have to work harder to make the case that an open Internet is and will be in everyone’s best interest” (Clinton 2011).

The Internet has been described as a “Playground for Political Liberalization” (Hofheinz 2005) in the MENA region. Based on the trade in censorship and surveillance technologies, it seems that the Internet was an extraordinarily dangerous playground filled with many seen and unseen risks for the users involved. Tunisia, Syria, Libya and Egypt all employed extensive technical measures to restrict the human rights of their populaces. These practises are by no means unusual in the MENA region, as the states involved seem keenly aware of the effects of losing control of communications technologies and took extensive measures to ensure continued control.

Market mechanisms responded to these demands and within a decade an industry has sprung up to provide censorship and surveillance technologies to authoritarian regimes in the MENA region and beyond (Silver and Elgin 2011). The international markets provide technology that is overwhelmingly developed in North America and Europe to authoritarian regimes worldwide (Noman and York 2011; King 2011). These market mechanisms also come into play when there are widespread public protests in a country. It seems that the signs of a popular revolution are interpreted as an opportunity for further business. An additional market clearly exists for censorship and surveillance technology provided at the last minute during popular uprisings. Although there is still significant regulation of encryption technology, there is very little existing regulation of censorship and surveillance technology. This has allowed the market to expand greatly in a relatively short time without any consideration of human rights concerns. Although public policy is slowly catching up, it remains several technology cycles behind the most recent developments in censorship and surveillance technologies.

Occasionally however there are instances when companies pull out of particularly controversial agreements. The most obvious case in this context is the European/U.S. consortium led by Area SpA (Silver 2011b). Following the publication and widespread condemnation of the Area case, several of the companies involved decided to abandon their Syrian surveillance project all together. While there are very few examples like this, there is some indication that sustained public pressure on industry players can produce meaningful results.

Popular uprisings in Middle East and North Africa provide an opening for states in Europe and North America to reconsider how they regulate the censorship and surveillance technologies exported to these countries. Both in Tunisia and beyond, the use of these technologies by authoritarian states to the detriment of their own population raises considerable human rights concerns. Prominent reports published in 2010 and 2011 by the OSCE, UNESCO, the Council of Europe and the Special Rapporteur on Freedom of Opinion and Expression Frank La Rue all emphasise the importance of freedom of expression on the Internet both in its own right and to guarantee other human rights (La Rue 2011; A/HRC/14/23). If it can be achieved to make it more difficult for authoritarian states to acquire censorship and surveillance technologies, this would be a substantive contribution to the pursuit of human rights on the Internet.

8) Bibliography

Abdulla, Rasha A. 2007. The Internet in the Arab world : Egypt and beyond. New York: Peter Lang.

Anon. 2011. “Final Declaration.” in Freedom Online: Joint Action for Free Expression on the Interne. Den Haag, The Netherlands: Ministry of Foreign Affairs of the Netherlands.

Bildt, Carl. 2011. “Carl Bildt’s remarks on Digital Authoritarianism.” Retrieved June 19, 2011 (http://www.sweden.gov.se/sb/d/14194/a/169246).

Chakchouk, Moez. 2011. “Towards the Development of Broadband Internet in Tunisia: New Challenges, Opportunities and Perspectives.” in 3rd Arab Bloggers Meeting. Tunis, Tunisia.

Clinton, Hillary. 2011. “Secretary Clinton on Internet Freedom.” in Freedom Online – Joint Action for Free Expression on the Internet. The Hague, Netherlands: Bureau of Democracy, Human Rights and Labor, U.S. Department of State.

Cowie, James. 2011. “What Libya Learned from Egypt - Renesys Blog.” Renesys. Retrieved April 3, 2011 (http://www.renesys.com/blog/2011/03/what-libya-learned-from-egypt.shtml).

Elgin, Ben, Vernon Silver, and Hermann Zschiegner. 2011. “Wired For Repression.” Bloomberg. Retrieved December 20, 2011 (http://www.bloomberg.com/data-visualization/wired-for-repression/).

Elgin, Ben, and Vernon Silver. 2011. “Syria Crackdown Gets Italy Firm’s Aid With U.S.-Europe Spy Gear.Html.” Bloomberg. Retrieved December 21, 2011 (http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html).

Esther Saoub. 2011. “Deutsche Abhörsoftware für Ägyptens Geheimdienst?” ARD-Hörfunkstudio Kairo. Retrieved August 28, 2011 (http://www.tagesschau.de/ausland/abhoersoftware100.html).

Filastò, Arturo. 2011. “Blue Coat device logs indicate the levels of censorship in Syria.” Retrieved December 17, 2011 (http://hellais.github.com/syria-censorship/).

Fontaine, Richard, and Will Rogers. 2011. Internet freedom a foreign policy imperative in the digital age. Washington, DC□:: Center for a New American Security.

Goldstein, Eric. 2011. “Dismantling the Machinery of Oppression: In Tunisia, the Police State Doubled as a Jobs Program.” Retrieved March 12, 2011 (http://www.hrw.org/en/news/2011/02/16/dismantling-machinery-oppression).

Guibourg, Clara. 2011. “Sweden ‘weakened’ EU sanctions against Syria - The Local.” The Local Europe AB. Retrieved December 14, 2011 (http://www.thelocal.se/37720/20111203/).

Hudson, Michael. 1991. “After the Gulf war□: prospects for democratization in the Arab world.” The Middle East journal The Middle East Journal.

Karr, Timothy. 2011. “one u.s. corporation’s role in egypt's brutal crackdown.” Huffington Post. Retrieved December 14, 2011 (http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html).

Karr, Timothy, and Clothilde Le Coz. 2011. “Corporations and the Arab Net Crackdown.” Foreign Policy in Focus. Retrieved September 24, 2011 (http://www.fpif.org/articles/corporations_and_the_arab_net_crackdown).

King, Eric. 2011. “Our response to EU consultation on legality of exporting surveillance and censorship technology.” Privacy International. Retrieved December 17, 2011 (https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology).

Krempl, Stefan. 2011. “Bundesregierung hält an Export von Überwachungssoftware fest.” heise online. Retrieved December 14, 2011 (http://www.heise.de/newsticker/meldung/Bundesregierung-haelt-an-Export-von-Ueberwachungssoftware-fest-1392507.html).

Krempl, Stefan. 2008. “Macht hoch die Firewall.” Retrieved March 13, 2011 (http://www.heise.de/ct/artikel/Macht-hoch-die-Firewall-291824.html).

Kroes, Neelie. 2011. “ICT for democracy: supporting a global current of change.” in Freedom Online – Joint Action for Free Expression on the Internet. The Hague, Netherlands.

Lake, Eli. 2009. “Iran prepared to track dissent on social networks.” Washington Times. Retrieved October 5, 2010 (http://www.washingtontimes.com/news/2009/jun/20/iran-has-tech-to-track-tweets-texts/).

Leichtfried, Jörg. 2011. “Newsletter September.” Retrieved December 14, 2011 (http://joerg-leichtfried.at/mep-jorg-leichtfried/newsletter/).

National Security Council (U.S.), and United States. Executive Office of the President. 2011. “International strategy for cyberspace prosperity, security, and openness in a networked world.”

Noman, Helmi, and Jillian C. York. 2011. West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011.

OpenNet Initiative. 2009. “Internet Filtering in Egypt.” Retrieved March 16, 2011 (http://opennet.net/sites/opennet.net/files/ONI_Egypt_2009.pdf).

OpenNet Initiative. 2009. “Internet Filtering in Tunisia.” Retrieved (http://opennet.net/research/profiles/tunisia).

Ragan, Steve. 2010. “Tunisian government harvesting usernames and passwords.” Retrieved January 13, 2011 (http://www.thetechherald.com/article.php/201101/6651/Tunisian-government-harvesting-usernames-and-passwords).

Reporters Without Borders. 2011. “World Report - Tunisia.” Retrieved March 16, 2011 (http://en.rsf.org/report-tunisia,164.html?annee=1991).

La Rue, Frank. 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.

Ryan, Yasmine. 2011. “Tunisia arrests bloggers and rapper.” Retrieved March 12, 2011 (http://english.aljazeera.net/news/africa/2011/01/20111718360234492.html).

DER SPIEGEL. 2011. “Waffenexporte: Regierung will Ausfuhr rüstungsrelevanter Güter erleichtern.” Retrieved December 14, 2011 (http://www.spiegel.de/politik/deutschland/0,1518,796115,00.html).

Silver, Vernon. 2011a. “Post-Revolt Tunisia Can Alter E-Mail With `Big Brother’ Software - Bloomberg.” Bloomberg. Retrieved December 14, 2011 (http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html).

Silver, Vernon. 2011b. “Italian Firm Said to Exit Syrian Monitoring Project - Bloomberg.” Bloomberg. Retrieved December 21, 2011 (http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html).

Silver, Vernon, and Ben Elgin. 2011. “Torture in Bahrain Becomes Routine With Help From Nokia Siemens.” Bloomberg. Retrieved August 28, 2011 (http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html).

Sonne, Paul, and Margaret Coker. 2011. “Foreign Firms Helped Gadhafi Spy on Libyans.” Wall Street Journal. Retrieved September 23, 2011 (http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html).

de Vreij, Hans. 2011. “EU wants stricter control of censorship software | Radio Netherlands Worldwide.” RNW. Retrieved September 23, 2011 (http://www.rnw.nl/english/article/eu-wants-stricter-control-censorship-software).

Wagner, Ben. 2008. “Deep Packet Inspection and Internet Censorship: International Convergence on an ‘ Integrated Technology of Control ’ 1.”in 3rd Annual Giganet Symposium, vol. 2. Hyderabad (Andra Pradesh), India.

Wagner, Ben. 2011. "'I Have Understood You': The Co-evolution of Expression and Control on the Internet, Television and Mobile Phones During the Jasmine Revolution in Tunisia." International Journal of Communication; Vol 5 (2011).

Waleed, Khaled. 2011. "What was Iraq's role in the export of banned US-made web watching gear to Syria?" Niqash: briefings from inside and across Iraq.

Contact

Humanist Institute for Cooperation
with Developing Countries (Hivos)
Raamweg 16 | P.O. Box 85565 | 2508 CG
The Hague | The Netherlands
T +31-70 376 55 00 | **F** +31-70 362 46 00
info@hivos.net | www.hivos.net

Courtesy of ANP