ENEMIES OF THE INTERNET

2013 REPORT

SPECIAL EDITION: SURVEILLANCE

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

ERA OF THE DIGITAL MERCENARIES

„My computer was arrested before I was.“ This perceptive comment was made by a Syrian activist who had been arrested and tortured by the Assad regime. Caught by means of online surveillance, Karim Taymour told a *Bloomberg* [1] journalist that, during interrogation, he was shown a stack of hundreds of pages of printouts of his Skype chats and files downloaded remotely from his computer hard drive. His torturers clearly knew as much as if they had been with him in his room, or more precisely, in his computer.

Online surveillance is a growing danger for journalists, bloggers, citizen-journalists and human rights defenders. The *Spyfiles* that WikiLeaks released in 2012 showed the extent of the surveillance market, its worth (more than 5 billion dollars) and the sophistication of its products.

Traditional surveillance has not completely disappeared. Policemen continue to lurk near Internet cafés in Eritrea. Vietnamese dissidents are followed and sometimes attacked by plainclothes policemen. The Chinese cyber-dissident Hu Jia and his wife Zeng Jinyang have had policemen stationed at the foot of their apartment building for months. Intelligence agencies still find it useful to tap the phones of over-curious journalists. But online surveillance has expanded the range of possibilities for governments.

This year's **„Enemies of the Internet“ report is focusing on surveillance** – all the monitoring and spying that is carried out in order to control dissidents and prevent the dissemination of sensitive information, activities designed to shore up governments and head off potential destabilization.

Today, 12 March, World Day Against Cyber-Censorship, we are publishing two lists. One is a list of **five „State Enemies of the Internet“, five countries whose governments are involved in active, intrusive surveillance of news providers**, resulting in grave violations of freedom of information and human rights. The five state enemies are **Syria, China, Iran, Bahrain** and **Vietnam**.

The other is a list of five **„Corporate Enemies of the Internet“**, five private-sector companies that are **„digital era mercenaries“.** The five companies chosen are **Gamma, Trovicor, Hacking Team, Amesys** and **Blue Coat**, but the list is not exhaustive and will be expanded in the coming months. They all sell products that are liable to be used by governments to violate human rights and freedom of information.

Their products have been or are being used to commit violations of human rights and freedom of information. If these companies decided to sell to authoritarian regimes, they must have known that their products could be used to spy on journalists, dissidents and netizens. If their digital surveillance products were sold to an authoritarian regime by an intermediary without their knowledge, their failure to keep track of the exports of their own software means they did not care if their technology was misused and did not care about the vulnerability of those who defend human rights.

Research by Bloomberg, the *Wall Street Journal* and the University of Toronto's Citizen Lab has established that surveillance technology used against dissidents and human rights defenders in such countries as Egypt, Bahrain and Libya came from western companies. Two types of corporate products are criticized in our report: on the one hand, equipment used for large-scale monitoring of the entire Internet, and on the other, spyware and other kinds of tools that permit targeted surveillance.

1 Read the „Hackers in Damascus“ article

This type of spyware is used to spy on the content of computer hard disks, recover passwords, access instant messaging content and monitor VoIP conversations. It can be installed on computers directly or remotely via the Internet, without the user noticing, by means of false updates or email attachments. Use of this kind of spyware by the private sector is limited. Some producers supply it directly to state agents such as intelligence and security services. Others openly advertise their software's ability to track down and spy on government opponents. Authoritarian regimes use it to spy on journalists and their sources and thereby suppress freedom of information.

Some surveillance technology can be used in two different ways. It can be used for the legitimate purpose of combating cyber-crime. And, in the hands of authoritarian regimes, it can be turned into formidable censorship and surveillance weapons against human rights defenders and independent news providers. The lack of legislation and oversight of trade in these "digital weapons" allows authoritarian governments to identify critical journalists and citizen-journalists and go after them.

Reporters Without Borders calls for the introduction of **controls on the export of surveillance software and hardware** to countries that flout fundamental rights. The private sector cannot be expected to police itself. Legislators must intervene. The European Union and the United States have already banned the export of surveillance technology to Iran and Syria. This praiseworthy initiative should not be an isolated one. European governments need to take a harmonized approach to controlling the export of surveillance technology. The Obama administration should also adopt legislation of this kind, legislation such as the proposed Global Online Freedom Act (GOFA).

Governments did already negotiate about the inclusion of surveillance technology into the most comprehensive international treaty on export controls, the Wassenaar Arrangement. Unfortunately, they did not yet put these negotiations into force, to help journalists, bloggers and activists around the world [1].

Democratic countries seem increasingly ready to yield to the siren song of the need for surveillance and cybersecurity at any cost. This is evident from all the potentially repressive legislation that is being adopted or proposed, legislation that would open the way for generalized surveillance. *FISAA* and *CISPA* in the United States, the *Communications Data Bill* in Britain, the Wetgeving Bestrijding Cybercrime in the Netherlands – they would all sacrifice online freedom of expression to combatting cyber-crime (for more information, see the „Overview of Cyber-censorship in 2012" chapter). If governments that traditionally respected human rights adopt this kind of repressive legislation, it will provide the leaders of authoritarian countries with arguments to use against the critics of their own legislative arsenals.

Increasingly widespread cyber-censorship and cyber-surveillance are endangering the Internet model that the Net's founders envisaged: the Internet as place of freedom, a place for exchanging information, content and opinions, a place that transcended frontiers. The Internet is also being threatened by the battles between governments for influence. Standardized surveillance is one of the leading calls of countries fighting for control of Internet governance. During the World Conference on International Telecommunications in Dubai last December, China backed a proposal aimed at dramatically extending ITU control over the Internet. With the support of Russia, Saudi Arabia, Algeria and Sudan, China called for the protection of the „physical and operational safety of networks", use of DPI in new generation networks [2] and an end to ICANN's management of domain name space and IP address spaces.

The situation is complex for news providers, who are torn between, on the one hand, the need to protect themselves and the safety of their sources while online and, on the other, the desire to gather and circulate information. Protection of sources is no longer just a matter of journalistic ethics; it increasingly also depends on the journalist's computer skills, as cyber-security specialist Chris Soghoian noted in an op-ed piece for the *New York Times*.

1 http://www.wassenaar.org/publicdocuments/2012/WA%20Plenary%20Public%20Statement%202012.pdf see also: https://www.privacyinternational.org/press-releases/british-government-welcomes-foreign-affairs-committee-recommendation-to-control

2 The December 2012 ITU summit in Dubai aimed to establish uniform Internet standards. One of the proposals at the conference was the standardized use of Deep Packet Inspection technology. This type of technology is extremely intrusive as it can be used to access the content of emails, intercept instant messaging and access all the content that a user has viewed while browsing.

If war reporters care about their physical safety, they take a helmet and bullet-proof vest when they venture into the field. Similarly, all journalists should equip themselves with a „digital survival kit" if they are exchanging sensitive information online or storing it on a computer or mobile phone. Reporters Without Borders is gradually developing such an Online survival kit on its WeFightCensorship website. It explains the need to purge files of their metadata, which give too much information away; it explains how to use the Tor network or Virtual Private Networks (VPNs) to anonymize communications; it offers advice on securing communications and data on mobile phones and laptops and so on.

Journalists and netizens must learn to evaluate the potential surveillance risks and identify the data and communications that need protecting in order to find appropriate solutions, preferably ones that are easy to use. The sophistication of the methods used by censors and intelligence agencies is testing the ingenuity of news providers and the *hactivists* who are ready to help them. But the future of freedom of information depends on the outcome of this battle. This is a battle without bombs, prison bars or blank inserts in newspapers, but if care is not taken, the enemies of the truth may sweep the board.

CORPORATE ENEMIES OF THE INTERNET

AMESYS (NOW BULL / AMESYS)

Amesys sold its EAGLE spyware to Libya while Muammar Gaddafi was still in power. It was used to spy on journalists and human rights activists there. As a result, the company is now being sued in France by the International Federation for Human Rights (FIDH) for complicity in torture. The lawsuit is still pending.w

Website: http://www.amesys.fr/
Country of origin: France

The company
Originally called i2e, Amesys is a French firm specializing in information technology that was founded in 1979. It was reorganized under the name of Amesys in 2004 and was taken over by the French technology company Bull in 2010. In 2011, a French-based NGO, FIDH, made a complaint regarding cases of complicity of torture [1]. In 2013, Amesys divested its EAGLE System to another company, Nexa Technologies. EAGLE is now being developed and marketed by a group of former Amesys employees led by Stéphane Salies, a former Bull director [2].

Portfolio
The EAGLE System allows government agencies to analyse web traffic, store the data and process it for later use by police or intelligence agencies.

„EAGLE core technology by AMESYS is designed to help law enforcement agencies and intelligence organizations to reduce crime levels, to protect from terrorism threats and to identify new incoming security danger.“ [3]

The system consists of a network probe, storage systems and monitoring centres for the purpose of analysis. The software allows for the creation of files on individual users, examples of which were found when anti-Gaddafi rebels raided the offices of Libya's secret police. EAGLE is based on Deep Packet Inspection technology and can analyse all kinds of web-related activities. The Amesys documentation lists the various kinds of online activity that can be inspected, including email (SMTP, POP, IMAP as well as webmail), Voice over IP, different chat protocols as well as http-web traffic and search engine queries.

Amesys involvement in Libya
Amesys products have been detected in Libya, where the company had a contract with Gaddafi's secret police. During a raid on offices of the secret police, Wall Street Journal reporters found EAGLE System manuals as well as individual files on Libyan citizens carrying the EAGLE logo.[4/5] Those spied on by the government included the Libyan journalist Khaled Mehiri. The Wall Street Journal reported [6] that the secret police had for months used Amesys tools to monitor Mehiri's emails (including his correspondence with Al Jazeera) and Facebook posts, printing out messages and storing them. In January 2011, as the Arab Spring was peaking in neighbouring Tunisia and unrest was building in Libya, Mehiri was summoned by intelligence officials and pressured not to publish statements by leading anti-Gaddafi activists. The surveillance continued thereafter. Fearing for his family's safety, he went into hiding for several months until the end of the war.

The role of Amesys in Libya is currently being investigated for complicity in torture in France as a result of a lawsuit brought by the Paris-based human rights NGO, FIDH, which is acting for five Libyan citizens who were spied on with the EAGLE System. [7]

„The court of appeal has confirmed that there was sufficient evidence to start investigating this matter, despite the road blocks erected by the Paris prosecutor's office, which was obviously reluctant to allow an impartial and independent inquiry," said Patrick Baudouin, FIDH honorary president, FIDH legal counsel and head of its legal action group.

1 http://www.fidh.org/FIDH-and-LDH-file-a-complaint
2 https://www.privacyinternational.org/blog/bull-quietly-offloads-controversial-surveillance-technology-after-libya-revelations also http://reflets.info/bull-vend-eagle-a-un-actionnaire-de-crescendo-qui-est-lactionnaire-principal-de-bull/
3 http://www.wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf
4 http://www.fidh.org/Amesys-Case-The-Investigation-12752 http://wikileaks.org/spyfiles/docs/amesys/105_homeland-security-program-technical-specification-public.html
5 http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html
6 http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html
7 http://www.fidh.org/Amesys-Case-The-Investigation-12752

In september 2011, Amesys made a press release related to the information published by several media regarding its activities in Libya. [8]

BLUE COAT

American Company Blue Coat, specialized in online security, is best known for its Internet censorship equipment. This equipment also allows for the supervision of journalists, netizens and their sources. Its censorship devices use Deep Packet Inspection, a technology employed by many western Internet Service Providers to manage network traffic and suppress unwanted connections.

Website: www.bluecoat.com
Country of origin: USA

The Company
Blue Coat is a large IT company based in Sunnyvale, California, that is best known for providing filtering and censorship devices for countries such as Syria and Burma. The company also provides network analysis systems called „Intelligence Centres", which are used by companies and governments to monitor online traffic and identify performance problems. They allow for the monitoring of individual online behaviour.

Portfolio
Blue Coat offers Deep Packet Inspection technology, which can be used to survey and censor the Internet. With DPI, it is possible to look into every single Internet Protocol packet and subject it to special treatment based on content (censored or banned words) or type (email, VoIP or BitTorrent Protocol). DPI not only threatens the principle of Net Neutrality, which Reporters Without Borders defends, but also the privacy of users. It makes single users identifiable and, in countries that flout the rule of law and violate human rights, often exposes them to arbitrary imprisonment, violence or even torture.

Blue Coat describes PacketShaper, one of their products as follows:

„It's your network. Own it. [...] PacketShaper analyzes and positively identifies traffic generated by hundreds of business and recreational applications. And thanks to its integration with WebPulse – Blue Coat's real-time web intelligence service – PacketShaper can even control application traffic by web content category. [...] PacketShaper makes it easy to collectively control related applications and content, while giving you precise tools to get granular where necessary." [9]

DPI is especially threatening to journalists, bloggers, activists and their sources, as it inhibits private, anonymous communication.

Blue Coat sells to government agencies as well as individual companies, which distinguishes it from most other companies mentioned in this report.

Critical appearances

Burma (Myanmar)
The presence of 13 Blue Coat devices in Burma was confirmed in 2011 [10]. Their presence was detected from the message that many Internet users encountered when they tried to browse the Internet. The message said:

„Dear Valued Customers,
On 17 October 2011, Due to the failure of SEA-ME-WE 3 submarine fibre optic cable, the Internet connection was unstable. It is being fixed by concerned personnel during this period, the Internet connection may be significantly slow and possibly offline sometimes. We will keep you informed accordingly and sincerely apologize for any inconvenience caused.
With regards,
Yatanarpon Teleport"

8 http://www.wcm.bull.com/internet/pr/new_rend.jsp?DocId=673289&lang=en

9 http://www.bluecoat.com/products/packetshaper

10 https://citizenlab.org/wp-content/uploads/2012/07/02-2011-behindbluecoatupdatefromburma.pdf

Shown in English and Burmese, the message had an URL in the address bar that began „notify.bluecoat.com", providing a good indication as to who was responsible.

Syria

In 2012, the Telecomix-Collective, a well-established hacker group that helped maintain connections to Egypt and other countries when governments tried to shut down access during the Arab Spring, released 54GB of logfiles which they say establish the presence of 15 Blue Coat proxy servers (Blue Coat Proxy SG9000) in Syria. These devices were discovered in the network of a state-owned ISP called the Syrian Telecommunications Establishment (STE). [1]

The crucial aspect for user privacy is that all attempts to connect to those services were logged and possibly investigated. Stephan Urbach of Telecomix says that there is evidence not only of logging and investigation of connection data, but also of investigation of the content submitted. [2]

The logs analysis suggests the Blue Coat proxy was used to intercept and analyse encrypted traffic (https). All the requests using the 443 port (dedicated to https traffic) and routed to some of the most visited websites [3] in Syria include more information than they should. That information is usually protected by an encryption layer that should prevent any kind of proxy from accessing it.

„‚We don't want our products to be used by the government of Syria or any other country embargoed by the United States', Blue Coat senior vice president Steve Daheb said in the company's first detailed explanation of the matter. He added that the company was ‚saddened by the human suffering and loss of human life' in Syria." [4]

In a Wall Street Journal report on 29 October 2011, Blue Coat acknowledged that 13 of its devices, initially shipped through a Dubai distributor and destined for the Iraqi Ministry of Communications, ended up in Syria. The company claimed in a statement that the devices were „not able to use Blue Coat's cloud-based WebPulse service" or „run the Blue Coat WebFilter database". Blue Coat also suggested that the devices were now „operating independently" and that the company did not have a „kill switch" to remotely disable them. The Citizen Lab led an investigation to verify the statements made by the company. It seems that indeed the Blue Coat devices in Syria do not anymore interact with the cloud services of the company [5].

Other appearances

In a major study, the University of Toronto's Citizen Lab scanned the Internet for Blue Coat devices around the world. [6]

Egypt, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates all reportedly use a Blue Coat system that could be used for digital censorship. Citizen Lab also determined that Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey and Venezuela also used equipment that could be used for surveillance and tracking. [7]

Reporters Without Borders contacted Blue Coat on 7 March. In a reply on 12 March, Blue Coat said its products were sold in accordance with the laws governing the sale of its technology. It said all of its sales were channelled through third parties and it expected the same compliance of them.

The misuse of technology to suppress freedom of expression or human rights was a serious issue, but not one that a single company could solve by itself, Blue Coat said, adding that it would engage with key stakeholders and other companies in the same industry in 2013 to identify what further steps it could take to limit misuse of its products.

---

1 http://online.wsj.com/article_email/SB10001424052970203687504577001911398596328-lMyQjAxMTAxMDIwODEyNDgyWj.html#

2 http://www.spiegel.de/netzwelt/netzpolitik/vorwurf-von-hackergruppe-syrien-soll-schnueffelsoftware-aus-usa-einsetzen-a-790834.html

3 The list of targeted websites: www.microsoft.com, imo.im, urs.microsoft.com, plusone.google.com, login.live.com, s-static.ak.facebook.com, www.facebook.com, secure.wlxrs.com, apis.google.com, by6.omega.contacts.msn.com, ssl.gstatic.com, www.google.com, mail.google.com, fbcdn-profile-a.akamaihd.net, login.yahoo.com

4 http://siliconangle.com/blog/2011/11/08/when-governments-curtail-freedom-a-tale-of-censorship-huawei-and-blue-coat/

5 https://citizenlab.org/2011/11/behind-blue-coat/

6 https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

7 http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html?_r=1&

GAMMA INTERNATIONAL

Gamma International offers advanced spyware, which has repeatedly been discovered in countries who mistreat journalists, like Bahrain and the United Arab Emirates. The Finfisher Technology sold by Gamma International is able to read encrypted files, emails and listen in to voice over IP calls. Among the targeted was Ala'a Shehabi, a journalist, university lecturer and activist from Bahrain, now living in London.

Website: www.finfisher.com,
https://www.gammagroup.com/
Country of origin: UK / Germany

The company

Gamma International is part of the UK-based Gamma Group, which specializes in surveillance and monitoring equipment (both on- and offline) as well as training services. Gamma has offices and subsidiaries in the United Kingdom, including the Channel Islands, and Germany, but also in Southeast Asia and the Middle East. [8]

Quote: *„The Gamma Group of companies, established in 1990, provides advanced technical surveillance, monitoring solutions, and advanced government training, as well as international consultancy to national and state intelligence departments and law enforcement agencies."* [9]

Gamma International is owned by Louthean John Alexander Nelson, son of Gamma Founder William Louthean Nelson, and Martin Johannes Münch (MJM). [10] Gamma is closely connected to German company Elaman ; the two companies are sharing an address and a phone number. Gamma has confirmed to Reporters Without Borders that Elaman is a retailer for its products.

Portfolio

Gamma International sells interception equipment to government and law enforcement agencies exclusively. Its FinFisher Suite (which includes Trojans to infect PCs, mobile phones, other consumer electronics and servers, as well as technical consulting) is regarded as one of the most advanced in today's market. A computer or smartphone is remotely infected by a Trojan, which is then controlled by government agencies through command and control servers. A computer can be infected via false update notifications of software, malicious emails or through physical access to a machine. Finfisher also offers technology to infect an entire Internet cafe in order to survey all possible users. When installed, it is almost impossible to safely remove the Trojan. Also, there are no safe ways to circumvent Finfisher on an infected machine.

The software is said to be able to bypass common methods and anti-virus detection. It can listen in to Skype talks, chats and encrypted emails and is even able to turn on a computer's microphone or webcam remotely. With FinFisher technology, it is even possible to gain access to encrypted files on a hard drive. Those Finfisher-features are promoted by the firm in different advertising videos. [11]

Involvement in Bahrain

In July 2012 news broke about a possible involvement of Finfisher Technology in Bahrain, where the situation for journalists is especially severe, and many are imprisoned or tortured. Bahraini journalist, activist and university lecturer Ala'a Shehabi, now residing in London, was sent infected emails, which she found to be suspicious. She forwarded them to experts for technical analysis. This led to the detection of signatures from Gamma's Finfisher Software.[12]

8 Gamma is a European-based company with its headquarters in the United Kingdom and subsidiary offices in Germany, the Middle East and Southeast Asia. [from https://www.gammagroup.com/default.aspx] For the Channel Islands see http://www.guardian.co.uk/uk/2012/nov/28/offshore-company-directors-military-intelligence

9 https://www.gammagroup.com/companyprofile.aspx

10 http://www.mushun.de/imprint.html, http://buggedplanet.info/index.php?title=NELSON,_LOUTHEAN_JOHN_ALEXANDER, http://s3.amazonaws.com/files.posterous.com/temp-2011-03-07/DBEJyIrixEbjnCeshsGDGlGeycClnodEbqkAHAIldczzIJpEpntFGxoxyEGF/Gamma_International_Gesellschafter.png.scaled1000.png?AWSAccessKeyId=AKIAJFZAE65UYRT34AOQ&Expires=1360660710&Signature=5cn38R5mReoxez%2FbneKlJnII9Bk%3D

11 http://tinyurl.com/werbungueberwachungI

12 http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

In a still ongoing process, Reporters Without Borders, together with Privacy International, the ECCHR, the Bahrain Centre for Human Rights and Bahrain Watch filed an OECD complaint, asking the National Contact Point in the United Kingdom to further investigate Gamma's possible involvement in Bahrain.

Martin Münch, Chief developer and soon to be human rights officer of Gamma, claims that Bahrain stole a demo version of the software, modified it and now uses it to spy on journalists and dissidents. [1] Eric King, head of research at Privacy International said: *„Integrating FinFisher in a country's network is not an easy task. It requires careful planning and physical installation of proxy's and command and control servers to work. Simply stealing a demo copy is incredibly unlikely as no county sophisticated enough to be able to re-purpose FinFisher would bother using a commercial trojan in the first place."* Bahrain Watch also obtained evidence that the FinFisher Servers in Bahrain receive regular updates. This is unlikely to happen if the software had been stolen.

Offer to Egypt

During a search of an Egyptian intelligence agency office in 2011, human rights activists found a contract proposal with an offering from Gamma International to sell FinFisher to Egypt. The company said that no deal has been made.

Other known appearances

Earlier this year, a study by Rapid7, an Internet security firm, identified FinSpy – the control software for FinFisher command-and-control servers – as being active in Australia, the Czech Republic, Estonia, Ethiopia, Indonesia, Latvia, Mongolia, Qatar, the UAE, and the United States.

„We have identified several more countries where FinSpy command and control servers were operating," said Citizen Lab, a University of Toronto institute that specialises in digital issues. „Scanning has thus far revealed two servers in Brunei, one in Turkmenistan's Ministry of Communications, two in Singapore, one in the Netherlands, a new server in Indonesia, and a new server in Bahrain." Citizen Lab also comments that some of the detected servers have been taken offline, after being discovered. [2]

HACKING TEAM

Hacking Team describes its lawful interception products as „offensive technology" and has been called into question over deliveries to Morocco and the United Arab Emirates. The company's „Remote Control System," called Da-Vinci, is able, it says, to break encryption on emails, files and Internet telephony protocols.

Subsidiaries: USA, Singapore
Employees: around 40
Website: http://www.hackingteam.it
Country of origin: Milan, Italy

1 http://bahrainwatch.org/blog/2013/02/06/uk-spyware-in-bahrain-companys-denials-called-into-question/ http://www.guardian.co.uk/world/2013/feb/02/uk-firm-spyware-bahrain

2 http://www.informationweek.com/security/vulnerabilities/finfisher-mobile-spyware-tracking-politi/240006620

The Company

Hacking Team is a Milan-based business offering „offensive" capabilities for law enforcement agencies on six continents. The company employs around 40 people in Milan. It has offices in Annapolis, USA, and Singapore. The company defines itself in these terms : *„Here in Hacking Team we believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities. Technology must empower, not hinder."*[3]

Portfolio

„Remote Control System is an IT stealth investigative tool for LEAs. (It is offensive security technology. It is spyware. It is a trojan horse. It is a bug. It is a monitoring tool. It is an attack tool. It is a tool for taking control of the endpoints, that is, the PCs)."[4]

Hacking Team's „DaVinci" Remote Control System is able, the company says, to break encryption and allow law enforcement agencies to monitor encrypted files and emails (even ones encrypted with PGP), Skype and other Voice over IP or chat communication. It allows identification of the target's location and relationships. It can also remotely activate microphones and cameras on a computer and works worldwide. Hacking Team claims that its software is able to monitor hundreds of thousands of computers at once, all over the country. Trojans are available for Windows, Mac, Linux, iOS, Android, Symbian and Blackberry. [5]

„In modern digital communications, encryption is widely employed to protect users from eavesdropping. ***Unfortunately, encryption also prevents law enforcement and intelligence*** *agencies from being able to monitor and prevent crimes and threats to the country security.*

Remote Control System (RCS) *is a solution designed to* ***evade encryption*** *by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable. For Governmental LEAs and Agencies ONLY. [Highlights by Reporters Without Borders]"*[6]

The companys spokesperson, Eric Rabe, said, without going into details, that the company is able to monitor how their software is being used by customers. [7]

Involvement in critical countries

The company says it does not sell its software to countries that abuse human rights and that the product is used in around 30 countries worldwide on five continents.

„Software developed by Hacking Team is sold exclusively to government agencies, and it is never sold to countries that international organizations including the European Union, NATO and the US have blacklisted. An external committee of legal experts reviews each proposed sale to assure compliance with our policies. Contracts with the government purchasers limit the permissible uses of our software. We monitor news media and other public communications such as blogs and Internet comment for reports of abuses and investigate when appropriate."

However, several media reports and research by IT security experts have found traces of Hacking Team software in countries that do not have a good record on democracy and human rights.

Involvement in Morocco

Hacking Team software was identified on the office computers of the Moroccan news website Mamfakinch just days after it received the 2012 Breaking Borders Award from Global Voices and Google. The malware was transmitted via an infected Word document that purportedly contained important confidential information.

3 http://www.hackingteam.it/index.php/about-us

4 Taken from Hacking Team presentation: http://www.wikileaks.org/spyfiles/docs/hacking-team/31_remote-control-system-v5-1.html

5 http://www.hackingteam.it/media/video/HT-DarkSecrets.flv [Maybe insert the video onsite via iFrame and a screenshot for the PDF], also http://www.hackingteam.it/images/stories/RCS2012.pdf

6 http://www.hackingteam.it/index.php/remote-control-system

7 http://www.spiegel.de/netzwelt/netzpolitik/eric-rabe-vom-hacking-team-trifft-auf-den-aktivisten-jacob-appelbaum-a-886744.html

Asked by Reporters Without Borders to comment on media reports that Hacking Team's software has been used in Morocco, the company's spokesperson did not deny that it had been deployed there:

„We take precautions to assure our software is not misused and we investigate cases suggesting it may have been. However, we do not disclose client names or the location of our clients." (via email)

United Arab Emirates

Morgan Marquis-Boire, a security expert, examined corrupted attachments in an email that was sent to Ahmed Mansoor, a blogger who is from the United Arab Emirates. He found strong indications that a Trojan it contained came from Hacking Team. His findings have been published by the Citizen Lab, a University of Toronto institute specialising in digital issues. [1]

TROVICOR

Trovicor is one of the largest providers of lawful interception equipment worldwide, claiming to equip more than 100 countries. The company has been questioned, in particular during a hearing before the European Parliament Subcommittee on Human Rights in 2010, with respect to engagement in Iran, but also in Bahrain and Syria, where torture and imprisonment of journalists and dissidents occurs on a regular basis, helped by Western technology.

Formerly known as Nokia Siemens Networks (until 2009) and Siemens AG, Division for Voice and Data recording. Owned by Johann Preinsberger through Ickehorn Asset Management.

Country of origin: Germany, Munich
Known branches: Switzerland, Dubai, Islamabad, Kuala Lumpur, Prague
Employees: around 170
Website: www.trovicor.com

Portfolio: Monitoring Centre, Lifecycle Management, Intelligence Platform

The company

Trovicor, formerly a branch of Siemens, Department for Voice and Data Recording (operating since 1993), is one of the leading suppliers of surveillance equipment worldwide. This former operational division of German company Siemens claims to equip more than 100 countries worldwide with lawful interception technology and their specialized monitoring centres. Siemens outsourced this chain of business to a newly established business, the joint venture Nokia Siemens Networks in 2007. In 2009, it was sold again to form the new company Trovicor, which is itself owned by an asset management company. [2] The new company vowed to fulfill all Nokia Siemens Networks maintenance contracts. Trovicor is a lead sponsor of 2013 ISS World in Prague, the world's biggest fair for surveillance and censorship equipment. [3]

„Monitoring centres are, in our view, more problematic [than standard lawful interception equipment] and have a risk of raising issues related to human rights that we are not adequately suited to address. Our core competency is not working with law enforcement agencies, who are not our typical customers. Those agencies could have an interest in expanding the capability of monitoring centres beyond the standards-based approach of lawful interception." (Barry French of Nokia Siemens Networks, testifying to the European Parliament) [4]

There are many hints that Trovicor is closely cooperating with other surveillance technology companies, which supply wider ranging solutions like Trojans.

„These [Trovicor] turn-key solutions are based on Trovicor's own innovative cores and designed for integrating best-in-class third party products providing the most flexible platform for the apprehension of criminals." [5]

1 http://munkschool.utoronto.ca/canadacentre/research/backdoors-are-forever/

2 http://www.nokiasiemensnetworks.com/news-events/press-room/statements/telecoms-and-human-rights, http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

3 http://www.issworldtraining.com/iss_mea/sponsors2.html

4 http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

5 http://www.issworldtraining.com/iss_mea/sponsors2.html

Portfolio

Trovicor monitoring centres are capable of intercepting all ETSI-standard communications. That means phone calls, text messages, Voice over IP calls (like Skype) and Internet traffic. Spying on hard drives is not possible. Trovicor also offers solutions that allow processing and analysis of vast amounts of data (intelligent platforms). The company explicitly offers Lifecycle Management technology, which means they offer first assessment of networks and Internet structure in a country, supply monitoring solutions and corresponding training for government officials. They also maintain and further develop their systems, even deploying new features on installed hardware. [6]

Involvement in Bahrain

Media reports as well as research by human rights groups around the world suggests that monitoring centres have been delivered to Bahrain and led to imprisonment and torture of activists and journalists. Sources from Trovicor (who formerly worked at Siemens) confirmed that technology was delivered by Siemens in 2006 and then maintained by its successor companies.

Prisoners like Abd al Ghani Khanjhar have been shown records of text messages, emails and intercepted phone calls during torture. This information could only have been obtained by the country's interception programme. [7]

Currently, Reporters Without Borders, together with the European Centre for Constitutional and Human Rights, Privacy International, the Bahrain Centre for Human Rights and Bahrain Watch, is pursuing an OECD complaint against the company at the German OECD National Contact Point to further investigate the company's involvement in Bahrain. [8]

Involvement in Iran

Nokia Siemens Network delivered lawful interception technology to Iran in 2009. When the company suspended monitoring centre business, Trovicor continued to maintain the monitoring centres. [9]

Nokia Siemens Networks still has a presence in Iran, providing assistance for mobile phone networks. At the end of 2011 the company announced they would reduce their presence in Iran. [10]

Other known appearances

Media reports state that Trovicor monitoring centre technology was delivered to Syria in 2000 and 2008. [11]

Yemen is said to have purchased Trovicor monitoring centres. In 2010 the company asked for trademark protection in Yemen, indicating that Trovicor does have interests in this country. [12]

Trovicor has an official branch in Kuala Lumpur, Malaysia. In 2009 the company asked for trademark protection in that country. [13]

Trovicor is also involved in Germany, where it is providing lawful interception for the state police of Bavaria (Landeskriminaltamt Bayern). [14]

---

6 http://trovicor.com/en/communication-monitoring-en.html, http://trovicor.de/en/our-offerings-en/lifecycle-management-en.html see also: http://trovicor.de/images/pdf/release_t01_2013.pdf

7 http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

8 http://en.rsf.org/bahrein-human-rights-organisations-filed-04-02-2013,44016.html

9 http://www.belgeler.com/blg/2ztn/nokia-siemens-monitoring-system-used-by-the-iranian-regime, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

10 http://www.itworld.com/networking/233025/nokia-siemens-scales-down-presence-iran

11 http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html

12 http://www.moit.gov.ye/moit/sites/default/files/%20%D8%A7%D9%84%D8%B9%D9%84%D8%A7%D9%85%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AA%D8%AC%D8%A7%D8%B1%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%A7%D8%AF%D9%8A%D8%A9%20%D8%A7%D9%8A%D8%AF%D8%A7%D8%B9_1.pdf , also http://www.abendblatt.de/politik/deutschland/article2003016/Folterer-in-Bahrain-profitieren-von-deutscher-Ueberwachungstechnik.html (German)

13 http://www.intellect-worldwide.com/welcome/documents/egazette/MY_eJournal/2010/25Nov2010-%28Jil.54No.24TMA-No.35%29.pdf

14 http://ted.europa.eu/udl?uri=TED:NOTICE:382568-2010:TEXT:EN:HTML&src=0&tabId=1

STATE ENEMIES OF THE INTERNET

BAHRAIN

The Internet in Bahrain

- Population: 1,250,000
- Number of Internet users: 960,000
- Internet penetration rate: 77%
- Number of journalists jailed: 2
- Number of netizens jailed: 1

Bahrain has one of the best levels of Internet coverage in the Middle East [1]. With an Internet penetration rate of 77%, most Bahrainis are connected. Connection speeds are fairly good (ranging from 512k to more than 20M, according to the region) and the number of Internet Service Providers is very high for the size of the population [2] (23 ISPs for 1.25 million inhabitants). Batelco, operated by the royal family, is the most important one [3].

Since 2011 and the start of the street protests, the Internet has proved to be a remarkable communication and information tool in Bahrain. Many Bahrainis have Internet access at home and activists use the good quality Internet connections to share ideas and files, whether via online media, blogs or social networks [4]. According to the latest Social Media Club study, the number of Twitter subscribers increased by 40% in the second half of 2012.

Online surveillance

While the speed of Bahrain's Internet connections is among the best in the Gulf, the level of Internet filtering and surveillance is one of the highest in the world. The royal family is represented in all areas of Internet management and has sophisticated tools at its disposal for spying on its subjects. Reporters Without Borders added Bahrain to its list of „Internet Enemies" in 2012. The situation for freedom of information has hardly improved since then amid the continuing street protests that began in February 2011 and were inspired by the uprisings in Tunisia and Egypt.

Activist community – organized but closely watched

Because of Internet filtering, a lot of online content is in theory inaccessible to the general public. The filtering obviously targets „pornographic" content but also and above all political and religious opinions that are at variance with the regime's. Content about the royal family, the government and Bahrain's Shiite community is strictly regulated although there are ways to circumvent the filtering.

The online activities of dissidents and news providers are closely monitored and the surveillance is increasing. According to Reda Al-Fardan, a member of the NGO Bahrain Watch, the Bahraini activist community is organized and active online, especially on social networks, but also very exposed. *„The number of attacks or emails containing malware has increased steadily since March 2012"*, he said.

Two kinds of cyber-attack have been identified:
- Malware sent as an email attachment
- IP address capturing

Phishing

Malware dissemination methods are becoming more and more pernicious. Reda Al-Fardan said: *„Those responsible for these attacks are becoming more and more intelligent and are using topics such as human rights and media freedom as baits."*

1 http://www.internetworldstats.com/stats5.htm
2 http://www-public.int-evry.fr/~maigron/RIR_Stats/RIPE_Allocations/IPv4/ByNb/BH.html
3 Viva, Batelco's main competitor, is owned by the Saudi royal family.
4 See the latest RWB report: http://12mars.rsf.org/i/Rapport_Ennemis_Internet_2012.pdf

The University of Toronto's Citizen Lab research centre intercepted some of these malware attachments and analysed their content and origin in a July 2012 report on Bahrain [5] which included an example of a widely-used phishing method:

----- Forwarded Message -----
From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

In the above example, the sender appears to be Melissa Chan, a real Al-Jazeera journalist, and the subject matter refers to mistreatment of Nabeel Rajab, the head of the Bahrain Centre for Human Rights, who was in prison in Bahrain at the time.

In the Citizen Lab report, software engineer Morgan Marquis-Boire analysed a piece of malware that was forwarded to Bloomberg journalist Vernon Silver by the Bahraini journalist and writer Ala'a Shehabi. The analysis established that the malware's originating IP address was at the headquarters of Bahrain's biggest ISP, Batelco, which is owned by the royal family.

IP address hacking

Twitter and Facebook account piracy is widespread. A „classic" *modus operandi* is used: bogus email accounts or bogus Twitter or Facebook accounts are created that are almost exact imitations of the accounts of dissidents. These bogus accounts are then used to send emails or tweets containing malware in the form of links. Whenever a dissident clicks on a link, the malware registers the IP address and captures the information in the dissident's account.

According to Bahrain Watch, the authorities can use an IP address to unmask the person behind an anonymous activist account. Once an IP address has been obtained – for example, when activists tweet directly from a mobile phone, as they often do, without using VPN or Tor or any other anonymization method – the authorities just have to search the files of the mobile phone companies, which have the IP addresses used by every client for their mobile Internet connections. The person behind an anonymous account is easily identified. Everyone in this person's network is then sent emails. And so it goes on. According to our sources, some of these attacks come directly from the government. Some dissidents have been arrested by the interior ministry shortly after clicking on one of these links.

Passwords demanded during interrogation

Although many dissidents have been arrested for demonstrating rather than expressing dissident views, the Bahrain Independent Commission of Inquiry's report said that, while detained, they were asked to identify their Facebook and Twitter contacts and to explain the reason for their membership of certain groups, the reasons for certain „likes" [6] and so on. It showed that their online activities were being very closely monitored. The government's opponents are not the only ones to be spied on. According to Bahrain Watch, the online activities of government supporters are also closely watched.

Ubiquitous royal family

In Bahrain, the royal family controls all of the entities that disseminate, monitor and regulate online information. As well as Batelco, the leading Internet Service Provider, members of the royal family also head the following influential bodies:

- IAA (Information Affairs Authority): The official name for the information ministry. Headed by Fawaz bin Mohammed Al Khalifa, a government minister and royal family member, the IAA has often been accused of censoring the Bahraini media, above all during the February 2011 protests [7].

5 https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf

6 http://files.bici.org.bh/BICIreportEN.pdf p.358

7 http://uncut.indexoncensorship.org/2012/01/bahrains-information-affairs-authority-censorshi/

The IAA controls the Bahrain News Agency and the Bahrain Radio and Television Corporation (the government's official mouthpieces), and actively monitors Al-Wasat [1] (the country's only independent newspaper) as well as visiting foreign reporters.

- CIO (Central Informatics and Communication Organization): Headed by royal family member Sheikh Salman Mohammed Al-Khalifa, the CIO manages the Bahraini Internet, its systems and data. Originally created as a citizen personal database, the CIO was given much more extensive powers by royal decree [2]. It now has authority over all the ISPs, including the power to withdraw an ISP's licence at any time and to access and control all of its online traffic. This means that, when an Internet user is identified, his or her browsing can be monitored. All of this without supervision by any independent body.

It is at the CIO that the Internet surveillance mechanisms are located. According to Citizen Lab, they include provision for DPI (see below), which makes it possible to intercept the communications of any Bahraini citizen.

- Ministry of Interior (MOI): As well as exercising direct control over the Central Informatics Organization, the MOI oversees another entity for combatting cyber-crime – the Directorate for Combatting Corruption and for Electronic and Economic Security. Created in September 2012, this unit urged the public to report „online smear campaigns tarnishing the reputation of national symbols and leading public figures". Aimed at combatting the „crime of defamation", especially on online social networks, the initiative led to the arrest of four people for „misuse of social networks" within the first month of its launch.

- TRA (Telecommunications Regulatory Authority): Headed by Mohamed Ahmed Al-Amer and Sheikh Hamed bin Mohamed bin Hamed Al-Khalifa, the TRA was responsible for the closure of VoIP sites such as NonoTalk and Seefcall in 2010 and 2011 on the grounds that they were illegal [3]. According to our sources, the TRA gives direct orders to ISPs to close or block access to websites that are deemed to be illegal.

- National Security Apparatus: An intelligence agency headed by Adel bin Khalifa bin Hamad Al-Fadhel, the NSA actively monitors dissidents and opposition members through their profiles on social networks. The NSA has been given greater powers [4] since 2010 and has been implicated in many cases of torture [5], including the torture of Karim Fakhrawi12, an Al-Wasat co-founder and member of its board, and the blogger Zakariya Rashid Hassan[6].

- E-Government Authority: Created with the aim of digitalizing all of the government's activities, the EGA also has the thinly disguised goal of gathering as much data as possible about the kingdom's citizens. On the CIO's initiative (then headed Sheikh Ahmed Bin Atteyatallah Al-Khalifa), the EGA has embarked on a vast online identification campaign, called the National Authentication Framework, to „facilitate access to services" for Internet users. In view of the royal family's presence everywhere in telecommunications management and surveillance, this initiative is very disturbing.

Technological surveillance arsenal

The Bahraini government seems to have equipped itself with all the latest surveillance software and hardware available on the market and is in a position to monitor the Internet at all levels.

- Blue Coat: In its Planet Blue Coat report, Citizen Lab identified a Deep Packet Inspection (DPI) tool produced by Blue Coat called PacketShaper. It is used to analyse and recognize Internet traffic and block access to certain kinds of content. According to one of the report's writers, Blue Coat is installed at the headquarters of the CIO, which manages the entire country's Internet.

1 http://www.bna.bh/portal/en/news/536417
2 http://www.bna.bh/portal/en/news/494535?date=2012-03-2
3 http://www.tra.org.bh/en/pdf/Nonotalk_order_press_statment_en.pdf
4 http://www.bahrainrights.org/en/node/3265
5 http://files.bici.org.bh/BICIreportEN.pdf pp. 243 à 245
6 http://fr.rsf.org/bahrein-le-fondateur-du-journal-al-wasat-18-04-2011,40036.html

- Gamma/FinFisher: Bahrain Watch and Citizen Lab have also demonstrated that a Gamma product called FinSpy, part of the FinFisher suite, was used in Bahrain. FinFisher products can potentially spy on any computer, control webcams and record all keystrokes, Skype conversations and even mobile phone conversations [7].

Gamma insists that the FinSpy product used in Bahrain was stolen [8]. It is surprising, to say the least, that a company specializing in computer security such Gamma allowed one of its own security products to be stolen during a demonstration. It is even more astonishing that the FinFisher products discovered in Bahrain by Citizen Lab were updated [9]. According to Bill Marczak, a member of Bahrain Watch and author of the Citizen Lab report on Bahrain, the FinSpy versions found in Bahrain in March 2012 were FinSpy 4.01 while FinSpy 4.00 had previously been identified.

- Trovicor: According to our sources, Bahrain has also had Trovicor products since the late 1990s. Like FinFisher, Trovicor's products can be used to monitor Internet conversations, mobile phone conversations and SMS. Other companies such as Nokia Siemens Networks have been told in the past to stop selling their tracking software in Bahrain[10]. NSN, whose datacentre was taken over by Trovicor, sold surveillance products that made it possible for the authorities to arrest and torture government opponents.

SmartFilter, a software programme sold by the US company McAfee, was also used in combination with DPI tools until 2011 [11].

Main freedom of information violations

Reporters Without Borders has followed a dramatic increase in violations of freedom of information in Bahrain during the past three years, dating back to before the start of the anti-government protests. The government's crackdown has been successful thanks to a news blackout made possible by an impressive arsenal of repressive measures and widespread surveillance, including the sidelining of foreign media, harassment of human rights activists, arrests and prosecutions of bloggers and netizens, and smear campaigns against free speech activists. Many journalists, netizens and members of human rights groups are currently in prison or facing jail terms because of a Tweet, article, photo or Facebook post.

The role played by news providers has been all the more important because many foreign journalists have been denied entry on arriving in Bahrain. Asem Al Ghamedi of *Al-Jazeera* [12], Nicholas Kristof of the *New-York Times* and a Frankfurter Allgemeine Zeitung [13] reporter were all turned back at the end of 2012. In some cases, officials claimed there had been procedural irregularities in the issuing of visas [14].

On 1 March 2013, the following were in prison of facing a jail term

Dr. Abduljalil Al-Singace, a human rights defender and blogger, was one of a total of 21 defendants who were given very long jail sentences on 22 June 2011 of charges of belonging to terrorist organizations and trying to overthrow the government. All possibilities of appeal have been exhausted, and Al-Singace is now serving a life sentence.

Ali Abdulemam was tried in absentia in the same case, receiving a 15-year-jail sentence. After the release of the Bassiouni report, the Bahraini judicial authorities ordered a new trial before an appeal court.

Ahmed Humaidan, a photojournalist who has won 143 international prizes [15], has been detained since 29 December 2012 for documenting human rights violations. While held, he has been tortured and forced to confess to a crime he insists he did not commit.

Hassan Salman Al-Ma'atooq: a photographer in prison since March 2011, is accused of falsifying photos of injured persons and circulating false photos and false reports.

7 http://www.bloomberg.com/news/2012-08-29/spyware-matching-finfisher-can-take-over-iphone-and-blackberry.html

8 http://www.guardian.co.uk/world/2013/feb/02/uk-firm-spyware-bahrain

9 http://bahrainwatch.org/blog/2013/02/06/uk-spyware-in-bahrain-companys-denials-called-into-question/

10 http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

11 http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html

12 http://thepeninsulaqatar.com/qatar/219431-al-jazeera-journalist-denied-entry-bahrain-rejects-charge.html

13 http://bahrainwatch.org/access/

14 http://byshr.org/?p=942

15 http://www.bahrainrights.org/en/node/5586

The many human rights defenders and news providers who have been the victims of government repression include, Nabeel Rajab, the president of the Bahrain Centre for Human Rights, and Said Yousif Al-Muhafdha, the centre's acting vice-president [1].

Netizens victims of violence and torture

The citizen-journalist Ahmed Ismail Hussain was killed while covering a peaceful demonstration in Salmabad on 31 March 2012. Those responsible are still not known. On the other hand, the authorities were clearly to blame for the deaths of **Karim Fakhrawi**, a co-founder of the newspaper Al-Wasat and member of its board, and **Zakariya Rashid Hassan**, a blogger. Both died in detention after being tortured.

Reporters Without Borders condemns such denial of justice. Two judicial masquerades in late 2012 again highlighted the way journalists are treated: the journalist Reem Khalifa's conviction without her lawyers being able to examine the case against her, and Lt. Sarah Al-Moosa's acquittal on a charge of torturing the journalist Nazeeha Saeed. After this acquittal, Reporters Without Borders formally asked the United Nations special rapporteur on the independence of judges and lawyers on 23 October [2] to examine the issue of impunity for those responsible for violence against journalists in Bahrain.

Technical solutions

Spyware such as FinFisher is widely used in Bahrain. The FinFisher suite is rarely detected by antivirus applications. The only way to protect against this kind of software is to take effective precautionary measures before a computer or mobile phone is infected.

- Do not install any software received by email.
- Install software from a website only when https is used. The risk of phishing is reduced when certificates guarantee the identity of an https page.
- Do not install software from an unfamiliar source, even when the installation is recommended by a window that has opened up on your screen.
- Systematically update your operating system and the software installed on your computer. Updates often address security flaws.
- Do not browse with Internet Explorer. As it is the most widely-used browser, more malware targets it. Use Firefox or Chrome instead.

Protecting online anonymity is another security challenge. Many dissidents who used Twitter anonymously were arrested after clicking on an innocent-looking link that sent them to a webpage designed to capture their IP address, which the authorities then used to obtain their identity from Internet access providers. Using a VPN or Tor prevents this by anonymizing your IP address.

There are many VPN providers. They include Astrill VPN, Pure VPN and HMA. The Guardian Project offers a range of applications that will protect anonymity and privacy while using an Android phone. They include Orbot, a mobile phone version of Tor.

The NGO Access Now has published a guide to protecting data and communications for Middle East residents, with a section dedicated to mobile phones.

Finally, Tails is an operating system designed to protect its user's anonymity. Run from a DVD or USB stick, it allows you to browse the Internet anonymously on almost any computer, and leaves no trace.

For more information, read our Online survival kit

1 http://fr.rsf.org/bahrein-nabeel-rajab-a-nouveau-emprisonne-10-07-2012,43003.html
2 http://www.tra.org.bh/en/pdf/Nonotalk_order_press_statment_en.pdf

CHINA

The Internet in China

- Population: 1.34 billion
- Number of Internet users: 564 million
- Internet penetration rate: 42.1 percent
- Number of journalists in prison: 30
- Number of netizens imprisoned: 60

The Chinese Communist Party runs one of the world's biggest digital empires, if not the biggest. In the Middle Kingdom, all Internet access is owned by the state, which is usually another way of saying the Party. Individuals and companies have to rent their broadband access from the Chinese state or a state-controlled company. The four national networks, CTNET, Chinanet, Cernet and CHINAGBN, are the backbone of the Internet in China. The network was restructured in 2008, leading to the emergence of three major national service providers, China Telecom, China Unicom and China Mobile, in all of which the state has a majority control. Public access to the Internet is delegated to regional companies.

In a report issued in January this year, the government's China Internet Network Information Center (CNNIC) claimed a penetration rate of 42.1 percent. It says China has 564 million Internet users, of whom 277 million access the Internet via a mobile device. Number of Facebook users has reached 63.5 million (an eight-fold increase in two years), Twitter users are now 35 million (a three-fold increase in three years). Estimated number of Weibo users is 504 million.

A DSL connection with a data rate of one megabit costs between $10 and $20 a month, depending on the province.

Surveillance of the network

A government matter

Many government departments are involved in censoring and monitoring the Web:

1) The Internet Affairs Bureau and the Centre for the Study of Public Opinion of the State Council Information Office (effectively the government)
2) The Internet Bureau and the Information and Public Opinion Bureau of the Publicity Department (formerly the Propaganda Department).
3) The Ministry of Industry and Information Technology (MIIT)
4) The Internet Information Security Supervision of the Ministry of Public Security
5) The Ministry of Industry and Information Technology's Internet Illegal Information Reporting Centre

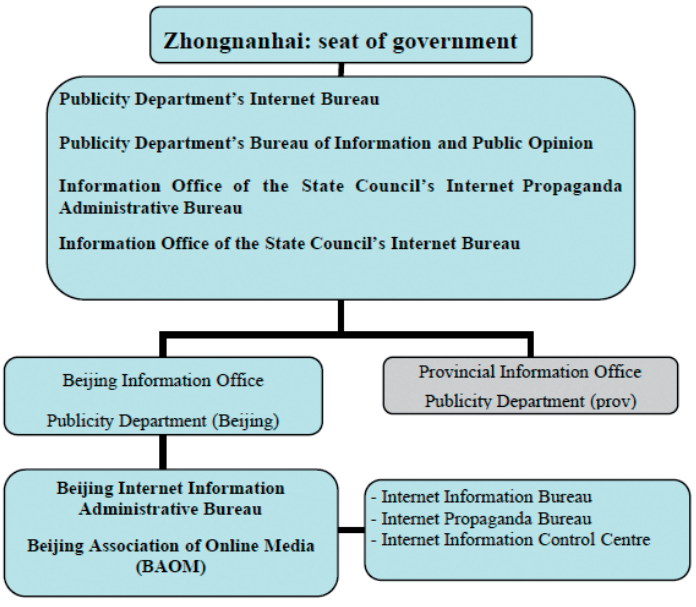


Table: Internet control bodies

The fourth and fifth of these bodies deal with issues of pornography, violence and computer fraud. The MIIT does not have direct control over the Internet. The bodies that have any real effect are the State Council Information Office and the Publicity Department.

The Great Firewall of China

The tools put in place to filter and monitor the Internet are collectively known as the *Great Firewall of China*. Begun in 2003, it allows access to foreign websites to be filtered. Besides the usual routing regulations that allow access to an IP address or a particular domain name to be blocked, the Great Firewall of China makes large-scale use of Deep Packet Inspection (DPI) technology to block access based on keyword detection.

According to a report entitled Planet Blue Coat by The Citizen Lab, an interdisciplinary research centre at the University of Toronto, at least three Blue Coat servers are used by the ISP China Net (controlled by the Chinese government) in Szechuan Province. Their presence was detected in late 2012. Blue Coat is a company that specialises in network surveillance products. The servers identified in China are of the PacketShaper type. They allow monitoring and control of Internet traffic by blocking feeds and content that are considered undesirable.

Access to circumvention tools

There are many ways of circumventing this Orwellian surveillance system, such as proxy servers, VPN, and Tor, but these are little used by ordinary Chinese.

Subscription VPN is not popular in China. It requires a credit card, which is an effective means of identification. Also, given that any company selling VPN services in China must register with the Ministry of Industry and Information Technology, using them can be even more risky.

Free workaround tools such as Tor or Freegate are constantly targeted by the authorities, which makes them slow and unstable. This means they are not used regularly. That leaves solutions provided by companies outside China. Until recently, these were the preferred alternative for Chinese citizens.

Great Firewall of China now plugged in

During the 18th Chinese Communist Party Congress last November, the Chinese authorities, keen to tighten their stranglehold on news and information, carried out a major upgrade of the Great Firewall. VPN services provided by non-Chinese companies were scrapped. The main users of foreign-hosted VPN had their connections cut.

The Great Firewall now has the ability to dynamically block encrypted connections. One of the country's main ISPs, China Unicorn, automatically cuts a connection as soon as it is used to transmit encrypted content.

Until now, only the VPN service of the company Astrill appears to allow Chinese citizens to pass through the Great Firewall and remain unidentified on the Internet. The other main VPN providers such as Witopia, StrongVPN and AirVPN remain blocked.

Workarounds blocked, netizens exposed

The use of VPN not only allows users to circumvent obstacles imposed by the authorities but also to conceal their IP addresses and encrypt their Internet communications. The main hitch caused by the upgrade of the Great Firewall and the blocking of all means of encryption is that this exposes Chinese journalists' and netizens' communications to the authorities' monitoring system.

Integrated monitoring system

The monitoring system developed by China is not confined to the Great Firewall, i.e. monitoring and blocking outgoing and incoming communications. Monitoring is also built into social networks, chat services and VoIP.

In China, private companies are directly responsible to the authorities for surveillance of their networks to ensure banned messages are not circulated.

The QQ application, owned by the firm Tencent, allows the authorities to monitor in detail exchanges between Internet users by seeking certain keywords and expressions. The author of each message can be identified by his or her user number. The QQ microblogging site is effectively a giant Trojan horse.

Since March last year, new legislation requires all new users of micro-blogging sites to register using their own name and telephone number. To force existing users to submit to scrutiny, the site Sina Weibo introduced a points-based permit two months later as part of its new user conditions. Each of Weibo's 300 million users is assigned an initial 80 points. A predetermined number of points is deducted for each violation of the conditions. When users have been stripped of all their points, their Weibo accounts are closed. Users on the verge of running out of points will be able to recover some if they spend two months without committing a violation or if they perform some unspecified promotional activity.

The highly popular WeChat mobile phone text and voice messaging communication service developed by Tencent changed its user conditions in February. Public users of the application, largely used by companies and celebrities, must now provide the number of their national identity card, their mobile telephone number and other personal information. They must also submit a copy of their identity card.

To ensure full control and put a stop to any attempt to prevent identification, the National People's Congress approved a rule requiring citizens who want to subscribe to Internet and phone services to provide their real identities.

TOM-Skype

It is not only social networks that are affected by these control measures. Skype, one of the world's most popular Internet telephone platforms, is closely monitored. Skype services in China are available through a local partner, the TOM media group. The Chinese-language version of Skype, known as TOM-Skype, is slightly different from the downloadable versions in other countries.

In order to conform to the restrictions imposed by the government, TOM-Skype software is equipped with an automatic filter. When certain keywords are detected in a text chat, the message is blocked and stored on an online server, according to a report by the OpenNet Initiative Asia. It said certain user names may also trigger the monitoring and interception of TOM-Skype text chats. The OpenNet Initiative Asia report also says everyday conversations are captured on servers. A sender's or recipient's name may be enough in itself to trigger the interception and storage of a conversation.

If workaround tools such as Tor or VPN are not used, the official Skye website (http://www.skype.com) redirects the user to the TOM-Skype website. The two sites are similar and some TOM-Skype users may not be aware that they are using a modified version of Skype and their security may be at risk.

In January this year, Reporters Without Borders and other NGOs sent an open letter to Skype asking it to clarify its relationship with TOM-Skype and to give details of the surveillance and censorship capabilities embedded in its software.

Foreign companies asked to help

The Quality Brands Protection Committee, which represents a number of multinational companies operating in China such as Apple, Nokia, Toyota and Audi, sent an email to its 216 members informing them of the Chinese authorities' concerns about the use of VPN by their employees in China to bypass the Great Firewall and communicate with other branches outside the country, and warning them they may be visited by the police. The email reported that the Chinese authorities were concerned about the use of VPN by multinational companies operating in China.

Police in Beijing, Hebei and Shandong were reported to have already asked some of these firms to install software allowing their networks to be monitored, on pain of having their Internet access cut off.

Collateral damage

A major impediment to the deployment of tools to monitor and control the network in China, aside from the issue of freedom of expression to which the Chinese pay little heed, is the economic impact of such measures on both Chinese and foreign companies. In the Internet age, surveillance is a cost that has an effect on business competitiveness.

Those who run online portals are frustrated by the time and energy invested in implementing censorship mechanisms. China's Web giant Tencent has to invest a huge sum in implementing censorship mechanisms in its online chat service. When the Great Firewall was upgraded, since when encrypted connections have been routinely blocked, many foreign companies operating in China that use VPN to access data outside the country have been penalised.

A recent example of the economic boundaries of censorship and control of the Chinese network concerns the biggest open-source hosting and repository platform, GitHub. GitHub hosts open-source software and numerous libraries of code that are invaluable for software developers.

After GitHub published a list of those who contributed code to the Great Firewall, and the large number of comments that ensued on the site, the Chinese authorities tried to block access to it. But GitHub uses the protocol https which prevents the authorities from blocking just the page containing the names of the Great Firewall contributors. Their other choice was to block access to the whole site, thereby denying access by Chinese companies working in the new technology sector to indispensible lines of code that it hosts, which was not an option.

Their only way of tackling the issue was a so-called „man-in-the-middle attack". A third party posing as a certification authority can interpose themselves between an https site and an individual user and intercept encrypted communications. This type of attack may not be obvious and most browsers, such as Chrome and Firefox, send security alerts to warn users when one is in progress.

The Chinese authorities use this system. On 26 January this year, Chinese Internet users who connected to GitHub received a warning that a third party was impersonating the site. The authorities' man-in-the-middle attack lasted ‚just an hour and was rather crude and easily identifiable. During that hour, however, any users who ignored their browsers' warnings could have been tracked, their IP address recorded and their passwords intercepted.

Internal and external surveillance

China has shown itself willing to extend surveillance beyond its own borders. On 30 January, the New York Times reported that it had been the target of attacks by the Chinese government. The first breach took place on 13 September 2012 when the newspaper was preparing to publish an article about the fortune amassed by the family of outgoing Prime Minister Wen Jiabao.

The newspaper said the purpose of attacks was to identify the sources that supplied the newspaper with information about corruption among the prime minister's entourage. The Wall Street Journal and CNN also said they had been the targets of cyber attacks from China. In February, Twitter disclosed that the accounts of some 250,000 subscribers had been the victims of attacks from China similar to those carried out on the New York Times.

Mandiant, the company engaged by the NYT to secure its nework, identified the source of the attacks as a group of hackers it called Advanced Persistant Threat 1. According to a Mandiant report, the group operated from a 12-storey building in the suburbs of Shanghai and had hundreds, possibly thousands, of staff. It is believed to have the direct support of the Chinese government and is a unit of the People's Liberation Army. While it is clear the attacks on the New York Times, the Washington Post and Twitter did take place and where they originated from, the debate sparked by the report by Mandiant, which also counts the U.S. government among its clients, has given the company unhoped-for media exposure. The boundary between a successful public relations campaign and a factual report is difficult to set.

Main violations in the country: emblematic cases of journalists or netizens arrested

China jails more people involved in news and information than any other country. Today 30 journalists and 69 netizens are in prison. Among them are several emblematic victims of the crackdown, which is subject to lulls as well as periods of tension, such as the start of the Arab spring and before and during last year's party Congress.

Many foreign journalists in China have told Reporters Without Borders that they take for granted that their telephones are tapped and their email is monitored. Local journalists also report that it has become more difficult for them to do their job. Many are suspicious of their foreign colleagues.

The cyber dissident Hu Jia served three-and-a-half years in prison for "inciting subversion". He was released in June 2011 but is still deprived of his civil rights and remains under house arrest. A few months after his release, the authorities seized his personal computer in order to retrieve his contacts and sensitive data.

In Tibet, there is now routine surveillance of Buddhist monks, among the last remaining conduits of information. The authorities have shown they are prepared to carry out raids on monasteries. On 1 September, 60 military vehicles descended on the Zilkar Monastery. Computers, DVDs, documents and photographs were seized from the monks' rooms.

During the night of 5 November, a few days before the party congress opened, the lawyer and blogger **Shu Xiangxin**, who specialises in land rights in the eastern province of Shandong, was arrested and his computer seized.

On 9 November, the blogger **Cheng Zuo Liang** was taken to the police headquarters in the eastern city of Ningbo for questioning about his links to a case involving the building of a polluting chemical plant. The police reminded Cheng he was banned from talking to Hu Jia during the party congress. The police also cited details from phone calls and emails between the two dissidents, confirming that Hu was under close police surveillance.

In April 2012, the artists and human rights campaigner Ai Weiwei, made a mockery of the surveillance arrangements by installing four webcams in his office and bedroom which filmed him around the clock. His web feed was shut down after a few hours.

Possible solutions

Websites such as GitHub, which are economically indispensible as well as performing a social function, present a real challenge to the Chinese authorities, who are unable to block or monitor them without penalising an entire section of the economy. This kind of service is a headache for China's Web monitors and provides a loophole for Chinese users of the Internet.

Other services such as repository services, servers that host the source code for Linux applications, have similar characteristics as GitHub and are an ideal way of getting past the Great Firewall, although they are difficult for non-developers to access.

Since the Great Firewall was upgraded, both subscription and free-of-charge VPN providers have developed their technologies still further. As of now, the free VPN available through Freegate still functions and can be used. As far as subscription software goes, Astrill has been the most responsive and its product is still able to circumvent the blockages in China.

This year the Chinese authorities have shown themselves to be responsive and that they know how to develop the Great Firewall to cope with major events such as the Bo Xilai scandal and the 18th party congress. It is a real cat-and-mouse game between government technicians and "hacktivists" or companies that offer data encryption and ways of circumventing the Great Firewall. In the words of a Freegate engineer, it is a matter of staying one step ahead and keeping future improvements in circumvention technology up one's sleeve. The main difficulty in this game is to provide journalists and netizens on the ground with the latest software.

For more information, read our Online survival kit.

IRAN

- Population: 77 million
- Number of Internet users: 25.2 million [1]
- Internet penetration rate: 32.8%
- Journalists in prison : 26
- Netizens in prison: 20
- Netizen killed in past year: 1

Iran has more than 150 Internet Service Providers or companies advertising themselves as such. Many of these services have been privatized since 2009 but that does not mean they have become fully independent of the government. The leading ones are still linked to the government and all are accountable to it. This biggest one, DCI, is owned by the Revolutionary Guards. Novinnet, Shatel, Asretelecom, Pardis, Persian-net, Tehrandat, Neda, Askiran and Tavana are the other leading ISPs.

Iranian Internet – fact and fiction

Iran has been connected to the Internet since the mid-1990s. For economic and political reasons, the authorities have developed the communications infrastructure to the point that Iran has the biggest number of Internet users [2] in the region. Iran's Internet depends on the Mullah regime, which controls infrastructure, technology and regulatory bodies, and has imposed repressive legislation.

While most Iranians get their news from television [3], the Internet plays a key role in circulating news and information thanks to dissidents and independent news providers. They report developments or views ignored by the traditional media, and cover government repression. The authorities often accuse social networks of being tools in the pay of western powers that are plotting against the government.

Internet connection speed has become an indicator of the political situation and the government alert level. On the eve of dates or anniversaries that could give rise to demonstrations, the connection speed is slowed right down to prevent the circulation of photos and videos. The Iranian Internet is not more politicized than in other countries, but it is definitely more closely watched. What marks it out is the fact that anything straying from the official line is automatically deemed to be „political" and subject to filtering or surveillance. Fashion, cuisine and music websites are often blocked just as opposition and independent news websites are.

„Halal Internet"

For the past decade, the government media have talked intermittently about the apparently insane project of creating „Our Own Internet" in Iran but it is finally beginning to take shape. The regime accelerated implementation in September 2012 on the grounds of a series of cyber-attacks on Iran's nuclear installations [4].

1 http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=graph

2 It should be noted that Iran's communication ministry often inflates the figures.

3 http://www.global.asc.upenn.edu/fileLibrary/PDFs/FindingaWay.pdf

4 http://fr.rsf.org/iran-lancement-imminent-de-l-internet-21-09-2012,43430.html

The construction of this parallel Internet, with a high connection speed but fully monitored and censored, is supposed to be completed in the very near future. It is intended that all Iranian websites will be hosted on local servers. Applications and services such as email, search engines and social networks are to be developed under government control [5]. This Intranet's imminent nationwide launch is disturbing. It will allow large-scale surveillance and the systematic elimination of dissent.

For the time being, only government offices are connected to the national Internet but it seems that the general public will eventually have no choice but to use it too. According to the information obtained by Reporters Without Borders, the government plans to reduce the international Internet's connection speed (which is already limited to 128Kb/s [6]) and to increase the cost of subscribing to it, in order to make subscribing to the faster national Internet much more attractive.

Technical surveillance

„In reference to the Computer Crime Law, access to the requested website is not possible."

The Islamic Republic of Iran possesses a technological and legislative arsenal that allows it to keep its Internet under close surveillance. Filtering, control of Internet Service Providers, prohibitions, and monitoring of email content, chats and VoIP conversations are all legal.

The complexity of Iran's internal politics and the approaching elections lend an additional opaque, unpredictable and at times apparently illogical character to the "legal" surveillance. The blocking of pro-regime websites and the outcry from government officials that followed the blocking of Google in Iran are examples of this.

„Official" surveillance and political infighting

The current political situation is such that it is almost impossible to determine the criteria for blocking content. The number of authorities, institutions, commissions and committees with responsibility for Internet management has grown ever since Mahmoud Ahmadinejad became president. They subject the Iranian Internet to an illogical and uncoordinated rollercoaster on the basis of often divergent political interests.

Internet Service Providers must register with the government and websites must get a licence from the Telecommunication Company of Iran (TCI). Blogs must also „register" with the Ministry of Culture and Islamic Guidance before being carefully scrutinized by the Working Group for Determining Criminal Content [7] and the Supreme Council for Cyberspace, which is headed by President Ahmadinejad and consists of government ministers, Revolutionary Guards and supporters of the Supreme Leader [8].

To ensure that online content does not contravene the spirit and „values of the Revolution", filtering is carried out at all levels by such means as blacklists, keywords, URLs [9] and IP addresses that are often shaped by internal political tension. Conservative opinion websites (such as Amir Hassan Sagha's blog and Mehdi Khazali's blog[10]) and pro-Ahmadinejad sites (such as the Shomanews website) are among those that have been blocked. Several pro-Ahmadinejad bloggers were prosecuted by the Tehran prosecutor's office in 2012 for criticizing supporters of Ayatollah Ali Khamenei. More and more journalists with conservative media are falling victim to the infighting between Khamenei and Ahmadinejad factions.

5 https://citizenlab.org/2012/11/irans-national-information-network/

6 http://www.lemonde.fr/proche-orient/article/2012/12/05/iraniens-encore-un-effort-pour-nationaliser-l-internet_1798592_3218.html

7 This committee reports to the Tehran prosecutor's office.

8 http://fr.rsf.org/iran-iran-12-03-2012,42014.html

9 List of blocked URLs: https://citizenlab.org/data/iranreport/

10 http://fr.rsf.org/iran-la-repression-sans-fin-du-regime-06-03-2012,42003.html

Censorship also affects less controversial subjects such as fashion or certain online games such as Travian [1]. And it goes without saying that keywords related to pornography are banned from search engines.

The Iranian authorities monitor access to both sites hosted abroad and those hosted in Iran. The sites of foreign media (both English and Persian-language media) are often blocked, or even copied or hijacked. The BBC, for example, discovered in January 2013 that Iranian Internet users trying to visit the bbcpersian.com website were being redirected to persianbbc.ir, whose content was much more in line with the values of the Revolution [2]. Similarly, the sites of Voice of America, Kaleme and Jaras cannot be accessed with circumvention tools.

Targeting social media

The head of the Iranian police, Esmaeil Ahmadi Moghadam, announced [3] in January 2013 that the government was developing technology that would enable better surveillance of social networks, above all Twitter and Facebook. By means of „intelligent control," it would be possible to „avoid the evils of social networks" while „benefitting from their useful applications", he said, presumably meaning that the Supreme Leader's Twitter account will be accessible but not those of government opponents or western journalists. Since government officials have a presence of social networks, Moghadam clearly thinks controlling them would be „more effective" than blocking them outright.

Although there are reasons for doubting Iran's ability to create the necessary infrastructure [4], the project is nonetheless disturbing, especially as the long blocked leading social networks such as Facebook and Twitter have been accessible again since 20 February 2013 [5]. Far from being a positive development, this probably signifies a new form of user surveillance.

Technical tools

The tools used by the Iranian authorities to monitor and control the Internet include not only filtering mechanisms but also, sources told Reporters Without Borders, data interception tools of the DPI (Deep Packet Inspection) type. Reports [6] and research have found Chinese products being used to monitor the Iranian population, products implicating leading Chinese companies such as ZTE [7] and Huawei [8]. The DPI provided by Huawei to Mobin Net, the leading national provider of mobile broadband, can be used to analyse email content, track browsing history and block access to sites. The products that ZTA sold to the Telecommunication Company of Iran (TCI) offer similar services plus the possibility of monitoring the mobile network [9].

European companies are the source of other spying and data analysis tools. Products designed by Ericsson [10] and Nokia Siemens Networks [11] (later Trovicor) have been detected. These companies sold SMS interception and user location products to Mobile Communication Company of Iran and Irancell, Iran's two biggest mobile phone companies, in 2009 [12]. They were used to identify Iranian citizens during the post-election uprising in 2009.

More astonishingly, the use of Israeli surveillance devices has also been detected in Iran. The network traffic management and surveillance device NetEnforcer was provided by Israel to Denmark and then resold to Iran [13]. Similarly, US equipment has found its way to Iran via the Chinese company ZTE [14]. As well as surveillance tools, the Iranian authorities use *man-in-the-middle* methods to prevent members of the public from using censorship circumvention techniques such as Tor, proxies and VPN [15].

1 http://www.bbc.co.uk/persian/science/2013/01/130104_na_travian_blocked_iran (Farsi)
2 http://www.guardian.co.uk/world/2013/jan/24/iran-fake-blog-smear-campaign-journalist-bbc
3 http://www.dw.de/intelligent-software-set-to-control-social-media/a-16507868
4 https://citizenlab.org/2013/01/middle-east-and-north-africa-cyberwatch-january-2013/
5 Reported on 1 March 2013
6 http://www.freedomhouse.org/sites/default/files/77_121312.pdf
7 http://www.reuters.com/article/2012/04/10/us-zte-iran-aryacell-idUSBRE8390T720120410
8 http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html
9 http://www.reuters.com/article/2012/12/05/us-huawei-iran-idUSBRE8B409820121205?utm
10 http://www.reuters.com/article/2012/11/20/us-iran-ericsson-idUSBRE8AJ0IY20121120
11 http://online.wsj.com/article/SB124562668777335653.html
12 http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html
13 http://www.bloomberg.com/news/2011-12-23/israel-didn-t-know-high-tech-gear-was-sent-to-iran-via-denmark.html
14 http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322
15 http://gallery.mailchimp.com/7fdb14e291091d23007369520/files/IIIP01.pdf

Powerful institutional apparatus

The government runs or controls almost all of the country's institutions for regulating, managing or legislating on telecommunications. The creation of the Supreme Council for Cyberspace in March 2012 showed how the government centralizes authority for Internet surveillance. This council now determines digital policy. The Supreme Leader appointed President Ahmadinejad to head it. The council has authority over Internet Service Providers. According to its general secretary, Mehdi Akhavan Behabadi, it is responsible for taking major decisions and coordinating Internet-related bodies.

When the sector was privatized in 2009, it was no surprise that the Revolutionary Guards' bid for the Telecommunication Company of Iran (TCI) was successful. The TCI owns the country's leading Internet Service Provider. The Revolutionary Guards also run the Centre for the Surveillance of Organized Crime and its official website Gerdab. The site has actively participated in tracking down netizens, calling on the public to denounce them [16]. The Revolutionary Guards also control the powerful Working Group for Determining Criminal Content and have thereby been responsible for a great deal of online censorship and arrests of independent news providers.

The Ministry of Culture and Islamic Guidance (MCIG), the Ministry of Intelligence and the Ministry of Information Technology and Communication also have a say in Internet surveillance and control but their decisions are affected by internal political rivalry. The MCIG, which is close to Ahmadinejad, recently asked mobile phone operators to screen for inappropriate text messages regarding the next elections [17]. This did not please all of the country's leaders because the Communication Regulation Authority qualified the announcement, saying that only „commercial" messages would be screened.

On February 26th Ahmadinejad named one of his lieutenants, Mohamed Hassan Nami [18], who has a doctorate in state management from the University of Pyongyang, in charge of the Ministry of Information Technology and Communication [19]. A North Korean-trained military officer is clearly unlikely to relax IT and communication legislation.

As well as these regulatory bodies, there is also a cyber-police force called the FETA. This body was responsible for a January 2012 decree imposing new regulations on Internet cafés, under which customers have to show ID and agree to being filmed by surveillance cameras, and managers are required keep the video recordings, full identity details and browsing history of customers for six months.

Increasingly repressive legislation

The 1979 Iranian constitution enshrines freedom of expression and prohibits surveillance except when provided for by the law. Article 25 says. *„Examination of (the contents of), and non-delivery of, letters; recording and divulging of telephone conversations; disclosure of telegraphic or telex communications; censorship, pruning or non-transmission of messages; tapping and bugging and any kind of investigation are all forbidden, unless when so ordered by the law."* Article 24 says: *„Publications and the press have freedom of expression except when there is infringement of the basic tenets of Islam or public rights [20]."*

The exceptions allowed by these two articles have been exploited to the hilt by the authorities. The 1986 press law, (amended in 2000 and 2009 to include online publications) allows the authorities to ensure that news providers do not *„attack the Islamic Republic", „insult the Supreme Leader"* or *„disseminate false information".* The amendments require online publications to obtain a licence.

The Islamic Republic crossed a new threshold in 2009, two weeks after President Ahmadinejad's disputed reelection, when it promulgated the Computer Crime Law (CCL). It provided for the creation of the Working Group for Determining Criminal Content, which now decides what does or does not comply with the Islamic Republic's laws (and therefore what may or may not be published). The CCL requires all ISPs to keep a record all data uploaded or downloaded by users, with severe penalties for failing to comply.

16 http://www.gerdab.ir/fa/pages/?cid=407

17 http://www.roozonline.com/persian/news/newsitem/archive/2013/january/14/article/-c463e593b1.html

18 http://www.president.ir/en/cabinet

19 http://articles.washingtonpost.com/2013-02-18/world/37155039_1_kim-il-sung-university-north-korea-key-post

20 Islamic Republic of Iran's constitution, Chapter 3, Articles 24 and 25.

Posting illegal content or using roundabout methods to access blocked content is punishable by long jail terms. The working group's members nonetheless do not agree on the illegal nature of circumvention tools such as VPN [1], and the Islamic Republic produces and sells its own so-called „halal" VPNs.

Main violations of freedom of information

The combination of these powerful technological arsenals, a legislative straitjacket and political infighting is an explosive mixture that demolishes the Iranian people's right to freedom of information. The start of 2013 has seen a wave of „preventive" arrests ahead of the June 2013 election. The regime clearly wants to head off widespread protests – relayed by the media and Internet – of the kind that accompanied the June 2009 election.

On 27 January 2013, now known as „Black Sunday", the authorities searched the offices of five Tehran-based newspapers (*Etemad, Arman, Shargh, Bahar* and *Aseman*), arrested 15 journalists (on or around that day), and announced that many other journalists would be summoned before tribunals [2]. Following surveillance by the Iranian intelligence agencies, these journalists are being accused of „collaborating with the West and counter-revolutionaries based abroad". Another dozen or so journalists, netizens, political activists and civil society representatives were summoned or arrested in the provinces three weeks later [3]. During interrogation, they were warned that any activities in connection with next June's presidential election would be met with reprisals. They were also asked to name their Facebook and Twitter contacts and give the reason for their relationships with them.

Ahmad Bakshaysh, a member of parliament's National Security Committee, told Roozonline on 18 February that the head of cultural affairs at the intelligence ministry had told him: *„These arrests are preventive. Their aim is to prevent the activities of a network inside and outside the country in the run-up to the June 2013 presidential election (…) This network encourages journalists to interview various government officials in order to highlight their differences (…) Since their arrest, some of them have understood their errors and are ready to testify to this (…) I think he was referring to televised confessions."* Reza Tajik, an Iranian journalist who is now a refugee in France, explained that, as well as spying on journalists and intimidating them, *„investigators subject journalists to psychological pressure during questioning so that they confess to espionage activities."* Tajik added: *„These confessions are filmed and then broadcast on TV."*

Mahmoud Ahmadinejad's second term as president has been marked by the surveillance and censorship of journalists and bloggers, in which many have been arrested. One blogger, Sattar Beheshti, who was jailed on 32 October 2012, died in detention in still unknown circumstances. The information available indicates that he died from blows received during interrogation. No one has been arrested for his death and no independent investigation has been carried out.

The regime tries to infiltrate journalist networks both inside and outside the country. Saeid Pourheydar, a journalist who was arrested in 2010 and mistreated during interrogation, said the intelligence officers who questioned him brandished transcripts of his phone conversations and printouts of his emails and SMS messages [4]. Fellow inmates told him they had had similar experiences. Such interrogation methods are widespread and are indicative of the degree to which journalists are spied on in Iran.

1 http://opennet.net/sites/opennet.net/files/iranreport2013.pdf pp. 20-21

2 http://fr.rsf.org/iran-le-guide-supreme-ali-khamenei-28-01-2013,43959.html

3 http://fr.rsf.org/iran-le-ministere-des-renseignements-20-02-2013,44098.html

4 http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

Journalists who have gone into exile or who are working abroad, especially those working for *Radio Free Europe* or the *BBC*, often receive emails containing malware. Some phishing attempts have been successful. When foreign journalists are allowed to visit Iran, their movements and their online activities are closely monitored. When they connect to the Iranian Internet, their data is immediately spied on if they fail to use secure communication and anonymization tools.

The repression will almost certainly keep on growing in the run-up to the June 2013 election.

Technical Solutions

Virtual Private Network (VPN)

Virtual Private Network technology (VPN) can be used to circumvent content blocking and censorship in Iran. The Iranian state sells this kind of technology in order to profit from the growing demand and to discourage netizens from getting it from abroad. Despite the Computer Crime Law (see above), it is legal to use an Iranian VPN in Iran. But foreign VPNs are forbidden. Nonetheless, they are the only ones that should be used. The Iranian state is not gullibly providing people with technology to circumvent its own censorship. The VPN provider is in a position to monitor and analyse all traffic through the VPN. While traffic is encrypted from the client's computer to the VPN server, it ceases to be encrypted between the server and the Internet. Those who control the VPN server (the Iranian authorities in the case of Iranian state VPNs) are completely free to observe and analyse traffic.

The Onion Router (Tor)

Tor is an anonymization tool that protects the user's private data while browsing. In Iran, Tor can be used when access to VPNs is blocked, but its use slows the browsing speed right down. Internet users prefer VPNs and regard Tor as a temporary alternative. Using Tor is banned and the Iranian authorities can ask Internet Service Providers to identify Tor traffic, which is easy to recognize and see where it is coming from. There is nonetheless a way to disguise Tor traffic: Obfsproxy. According to its developers, ISPs cannot detect Tor traffic when Obfsproxy is running.

Tips

The Iranian government's surveillance resources are changing all the time so the advice given below should be used with care because, while valid today, it may not be tomorrow. Keeping abreast of developments and the dangers to which you are exposed is therefore essential in order to adopt appropriate solutions.

- Do not use Iranian VPNs. Using a VPN controlled by the Iranian authorities is not a good idea. Soon or later it will be like throwing yourself into the lion's jaws.
- The regime does not yet have the resources for keeping millions of Internet users under surveillance. You should be able to fend off most threats if you adopt basic precautions such as regularly updating your operating system and software applications, using antivirus and VPN software, and systematically using the HTTPS protocol whenever possible.
- Basic „electronic hygiene" should prevent your computer from being infected by spyware: do not clinks on links from an unknown sender; do not download software when you do not know the sources; do not accept contact requests from strangers on social networks; and always identify the sender of an email before opening any attachment.
- When long blocked websites such as Facebook, YouTube or Twitter are suddenly accessible again, it will often be because the authorities are trying to use a man-in-the-middle attack to capture users' names and passwords. Using a VPN not only allows you to circumvent censorship; it also and above all allows you to elude network surveillance by encrypting all communication between you and the VPN server.

SYRIA

Syria, which Reporters Without Borders has already listed as an „Internet Enemy," has stepped up web censorship and cyber-monitoring as the country's conflict has intensified.

Since the uprising began on 15 March 2011, the regime has deployed systems designed to prevent the spread of news and images documenting the official campaign to crush the rebellion. An ultra-centralized internet architecture allows the government to cut off the country from the rest of the world, a step that authorities took on 29 November 2012 and which lasted two days.

The Internet in Syria [1]

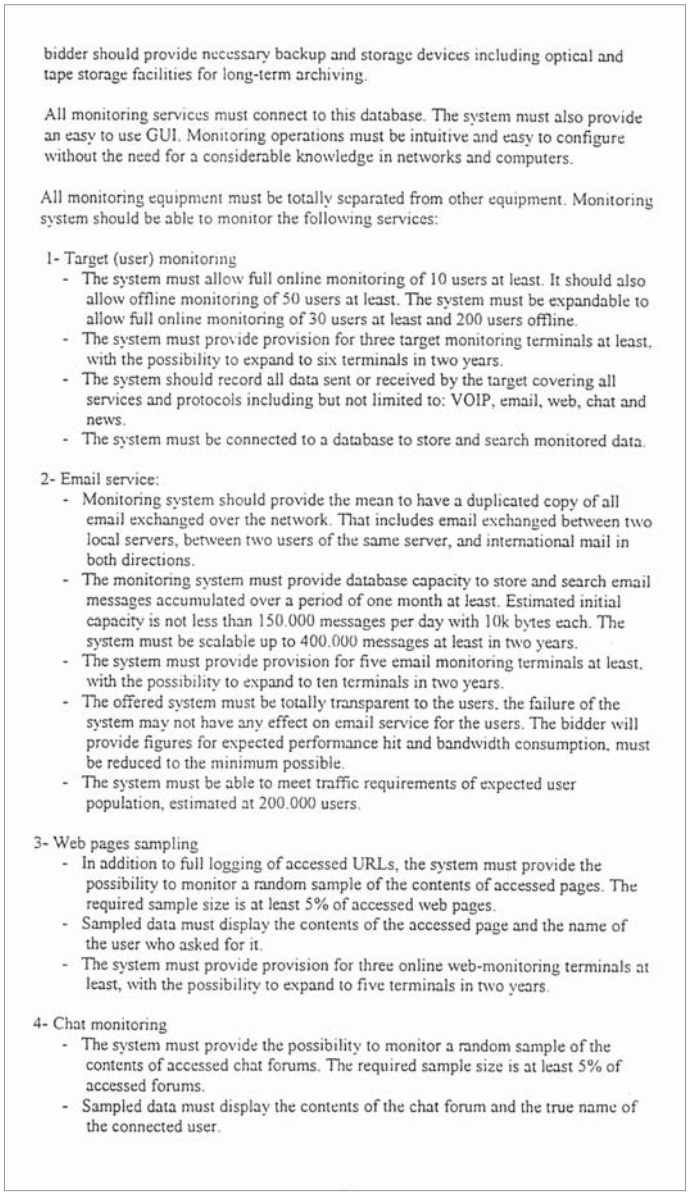
Population: 22 500 000
Number of Internet users: 5 000 000
Internet penetration rate: 22.5%
Journalists jailed: 22
Netizens jailed: 18
Netizens killed in 2012: 18

A network designed for filtering and monitoring

The Syrian internet network is controlled by two entities: the Syrian Computer Society (SCS) and the Syrian Telecommunications Establishment (STE).

Founded by Bashar Al-Assad, SCS controls Syria's 3G infrastructure. STE, from within the Telecommunications and Technology Ministry, controls the majority of fixed connections. The agency has granted ADSL operators the use of its cables. Alternatively, users connect via landlines and 56K modems. STE manages all web connectivity within Syria. When the government orders blocking of a word, of a URL or of a site, STE transmits the order to service providers.

Reporters Without Borders has obtained a confidential document: a 1999 bid invitation from STE to install a national internet system in Syria. The document makes clear that the system's capabilities were intended from the very beginning to include filtering and monitoring functions



bidder should provide necessary backup and storage devices including optical and tape storage facilities for long-term archiving.

All monitoring services must connect to this database. The system must also provide an easy to use GUI. Monitoring operations must be intuitive and easy to configure without the need for a considerable knowledge in networks and computers.

All monitoring equipment must be totally separated from other equipment. Monitoring system should be able to monitor the following services:

1- Target (user) monitoring
- The system must allow full online monitoring of 10 users at least. It should also allow offline monitoring of 50 users at least. The system must be expandable to allow full online monitoring of 30 users at least and 200 users offline.
- The system must provide provision for three target monitoring terminals at least, with the possibility to expand to six terminals in two years.
- The system should record all data sent or received by the target covering all services and protocols including but not limited to: VOIP, email, web, chat and news.
- The system must be connected to a database to store and search monitored data.

2- Email service:
- Monitoring system should provide the mean to have a duplicated copy of all email exchanged over the network. That includes email exchanged between two local servers, between two users of the same server, and international mail in both directions.
- The monitoring system must provide database capacity to store and search email messages accumulated over a period of one month at least. Estimated initial capacity is not less than 150.000 messages per day with 10k bytes each. The system must be scalable up to 400.000 messages at least in two years.
- The system must provide provision for five email monitoring terminals at least, with the possibility to expand to ten terminals in two years.
- The offered system must be totally transparent to the users, the failure of the system may not have any effect on email service for the users. The bidder will provide figures for expected performance hit and bandwidth consumption, must be reduced to the minimum possible.
- The system must be able to meet traffic requirements of expected user population, estimated at 200.000 users.

3- Web pages sampling
- In addition to full logging of accessed URLs, the system must provide the possibility to monitor a random sample of the contents of accessed pages. The required sample size is at least 5% of accessed web pages.
- Sampled data must display the contents of the accessed page and the name of the user who asked for it.
- The system must provide provision for three online web-monitoring terminals at least, with the possibility to expand to five terminals in two years.

4- Chat monitoring
- The system must provide the possibility to monitor a random sample of the contents of accessed chat forums. The required sample size is at least 5% of accessed forums.
- Sampled data must display the contents of the chat forum and the true name of the connected user.

The general description of the project (5.1) specifies that STE shall be the only entity providing internet connectivity. The bid invitation requires the future service provider to install filtering and internet traffic inspection systems at the heart of the network. The *Monitoring system* chapter (6-1-8) details an STE requirement that all questions to search engines be stored in a database for one month.

1 Source: Internet World Stats

The same chapter lists monitoring system requirements:

1) Recording of online and offline activities – VIP, chat, surfing and email – of approximately 60 specified individuals.
2) Capabilities must include copying of all email exchanges from within Syria.
3) The URLs of all web pages visited to be recorded.
4) Ability to gather a random sample of the content of posts to forums, which must disclose the senders' real names.
5) „Newsgroups" – now outmoded but heavily used in 1999 – also fall within the surveillance parameters.

System requirements also include the ability to detect, intercept and block any encrypted data.

It is impossible to know if the system installed in Syria in the early 2000s meets each of the wildly excessive requirements laid out in the bid invitation. But the document in any case makes clear the extent of official determination to monitor the entire internet system.

Refinement of filtering and monitoring systems

In 2011, the government added new technologies to its cyber-arsenal. The reflets.info site, working with the Telecomix digital activist group and a Tunisian portal, fhimt.com, revealed the presence of Blue Coat proxy servers in Syria. Evidence is posted on the site in the form of a scan of the Syrian network. The data is compiled in a digital file that is freely accessible for analysis.

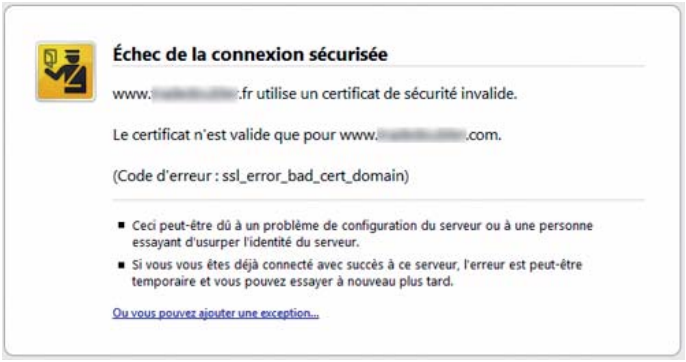
Originally, Blue Coat Systems Inc. denied having sold proxies to the Syrian government. After reflets.info posted the evidence, Blue Coat admitted the presence of at least 13 of its servers in Syria. These were apparently sold by a Dubai-based firm whose business was reselling and installing Blue Coat solutions.

In December 2011, Blue Coat announced that it would no longer provide support or updates for servers installed in Syria. The company also said it did not have the means to remotely de-activate servers. Network tests conducted in July 2012 by Citizen Lab showed that Blue Coat servers in Syria were no longer communicating with the parent firm, a finding that confirms the company's claim.

Chronology of *Man in the Middle* Attacks

February 2011 – As the Arab Spring uprisings begin, the Syrian government reopens access to sites - blocked for years - that are enabling Tunisians and Egyptians to mobilize: YouTube, Facebook, Twitter.

May 2011 – The Electronic Frontier Foundation, an NGO that defends digital-access rights, reports the first Man in the Middle (MITM)[2] attack. It is aimed at Syrians connecting to each other on the secure version of Facebook (see Lexicon). The users see alerts on their browsers warning that the certificate certifying a site's identity is not valid. Those who connect despite the warning have allowed the attackers to retrieve their user names and passwords.



A security warning on the Firefox browser during an MITM attack

July 2011 – Digital certification firm DigiNotar detects a network intrusion.

July-August 2011 – Hacktivist[2] group Telecomix launches #OpSyria and recovers more than 54 gigabytes of data on operation of the Blue Coat servers.

August 2011 – The https versions of Facebook and Yahoo! are blocked in Syria and automatically redirected to insecure versions. Users trying to connect to the sites are forced to disclose their passwords. The tactic means that users who don't know how to check that a site is secure lose their digital protection. Security indicators are a letter 's' in the URL (https), and the adjoining logo of a padlock.

2 See lexicon

August 2011 – Google detects use of a fraudulent DigiNotar certificate in Iran.

Files recovered through #OpSyria show that Syrian authorities have deployed extremely advanced MITM attacks. Blue Coat server connection logs normally should not record information after a user accesses a secure site (https). However, the connection logs show that Blue Coat servers did, in fact, register an abnormally large quantity of data not normally available due to encryption, following user access to sites that see the heaviest traffic in Syria. The theft of DigiNotar certificates likely explains this result.

Targeted attacks

The Syrian government's digital weapon includes more than Internet traffic analysis tools. Bloomberg and Citizen Lab report that authorities are also capable of targeted monitoring.

Lessons from an arrest: Taymour Karim

In „The Hackers of Damascus" journalist Stephan Faris of *Bloomberg Businessweek* reports the story of Taymour Karim, a Syrian activist arrested and tortured by the regime. Police picked him up on 26 December 2011, as he was on his way to a meeting with one of his contacts. The two had arranged the meeting on a Skype call.

But the authorities had monitored the call. Karim was detained for 71 days. Under interrogation, after he refused to disclose his activities and contacts, he was shown more than 1,000 pages of conversation transcripts and files, all gathered from Skype exchanges. Despite Karim's resistance, his interrogators had already gathered much of what they wanted to know from the digital trail that he had unwittingly left.

In January 2012, less than one month after Karim was freed, Morgan Marquis-Boire, a security expert at Google, examined the computer of an NGO member based in Syria. The activist thought its system had been compromised. An in-depth analysis showed that the activist was correct. The first intrusion had occurred on 26 December, only a few hours after Karim's arrest.

Spyware had been transmitted to the NGO member via a Skype message from none other than Karim. The software had been hidden in a document that Karim had finished the day before his arrest.

Phishing and social engineering

The Karim case displays the Syrian government's methods of monitoring and arresting netizens. Most commonly, during a Skype conversation, a contact suggests that the person on the other end of the call download a video, a document or an image.

The link that starts the download contains spyware. Once the user clicks it, the software installs itself. Skype accounts used in this fashion are those of netizens who have been arrested, or whose computers have been compromised. Accounts created for the specific purpose of trapping netizens have also been used.

Blackshade, a virus-infection campaign named after the malware it employed, was launched in Syria in June 2012. It was exposed thanks to a message from a compromised Skype account to a member of the Syrian opposition.

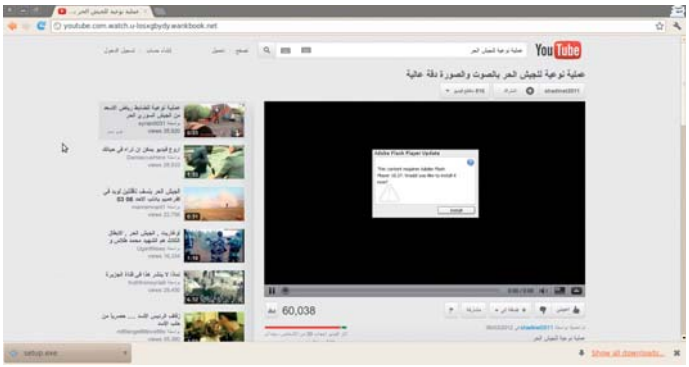
السلام عليكم
في شخص بيكرهك وعم يجيب سيرتك وانا صورت المحادثة باريت الانتباه من هذا الشخص وبيعرفك شخصي
هذه صورة عن المحادثة
http://14wre.co.za/new.zip

Screenshot from the EFF article on Blackshade (Creative Commons License

In translation, the message reads: „There is a person who hates you, and keeps talking about you. I took a screenshot of the conversation. Please beware of this person, as he knows you personally. This is a screenshot of the conversation." After the message recipient clicks on the included link, the malware installs itself.

The regime also uses a variety of phishing tactics. One of them involves producing a copy of a known site, such as YouTube or Facebook, and demanding that the user enter personal information for seemingly legitimate reasons. These can include updating a profile, or agreeing to a new confidentiality policy.

In March, a counterfeit YouTube site said to host opposition videos required users to enter their log-in and password in order to register comments. The site also enabled installation of spyware by asking those connecting to download an update to Adobe Flash (software that enables viewing of online videos).



Screenshot from EFF article (Creative Commons License)\

In April 2012, EFF identified at least five phishing attempts aimed at Facebook users. One was transmitted by messages left on Facebook accounts of Syrian opposition leaders, including Burhan Ghalioun. Clicking on the links posted on these pages sent the user to a false Facebook page, which offered installation of an application, FacebookWebBrowser.exe, supposedly designed to improve Facebook account security.

In fact, FacebookWebBrowser.exe is spyware that enables the capture of all characters typed on a keyboard, as well as usernames and passwords for email, YouTube and Skype.

In August 2012, EFF spotted another spyware launch. This campaign centred on a program named *Antihacker*, billed as way to protect the computer in which it was installed. The program installs a version of DarkComet, a program that can record images via the webcam of the victim's device, de-activate warnings from certain anti-virus programs, record keyboard strokes and retrieve passwords.

Install screen of the ill-named AntiHacker

Most targeted attacks have been carried out using certain RAT [3] spyware programs – DarkComet or BlackShade. Once installed on a computer or mobile device, these programs grant access to the webcam, to email passwords, YouTube, Facebook, Skype conversations and keyboard strokes.

Information captured by these malware programs is sent to servers with Syrian IP addresses. The reasonable conclusion is that the attacks originate with the same group - the Syrian Electronic Army.

This pro-government organization likely also devised the false YouTube page used in the phishing campaign described above. In July 2012, the Electronic Army disseminated 11,000 names and passwords of „NATO supporters" – that is, opposition members.

According to some experts, the paramilitary group works closely with Syrian intelligence services.

3 See lexicon

Potential Solutions

Protecting against malware is essential in Syria, given the constant threat posed by these programs.

Computer protection

The key is to follow basic guidelines:

- Do not install any software received by email.
- Do not install any software unless it is downloaded from an https site. The risk of falling victim to phishing is lessened when a site with a certified identity is used.
- Do not install any software from an unfamiliar source, even if installation is recommended in a window that suddenly appears.
- Systematically carry out updates of your operating system and software. Updates frequently resolve security issues.
- Do not use Internet Explorer. As the most popular browser, it is a major target for hackers. Use Firefox or Chrome instead.

Protect your browsing and guard against MITM

The simplest anti-MITM measure is to *not ignore security warnings* from a browser when connecting to an https site. Chrome and Firefox offer extensions that detect MITM attacks.

https everywhere

This extension verifies on each site that an https version (encrypted) exists. If that is the case, the user is redirected to the secure site. Several scenarios are possible:

- If a phishing attempt targets Facebook users, those who have installed the extension are redirected to the https version.
- If the attack is a simple one, the user is sent to the genuine https Facebook site.
- In the case of a sophisticated attack that uses a counterfeit https site for phishing, users will receive a security alert notifying them that the site is counterfeit.
- In the case of highly sophisticated attacks, in which the attackers have compromised Facebook's certificate, the certificate has to be authenticated manually.

Https everywhere is useful on a daily basis. Every time a user transmits data, for example when filling out a form, it is essential to use the https protocol rather than http. Failure to do so means that all data will be transmitted unencrypted, to the user's peril.

Certificate Patrol

This extension verifies certificates – a site's ID papers – when a user lands on an https site. The user is alerted when a certificate is changed. This tool is indispensable to protect against MITM attacks. And it ensures that https requests are correctly encrypted.

VPN and TOR

Use of VPN (Virtual Private Network) or Tor provide effective protection against MITM and phishing attacks. These tools allow a user to bypass the Syrian network – thereby evading attacks mounted there – and to connect to the web in Sweden, the United States or elsewhere.

These tools are especially good at defeating monitoring because they mask users' IP addresses. VPN solutions have the added benefit of data encryption. Tor, for its part, simply anonymizes the user.

For more information, read our Online survival kit

VIETNAM

Vietnamese authorities face a dilemma common to authoritarian systems. The desire for economic development that builds on the new technologies [1] clashes with fear of political instability growing out of digital activism.

Internet in Vietnam (2012) [2]:

- Population: 91,500,000
- Number of Internet users: 31,000,000
- Internet penetration rate: 33.9%
- Imprisoned journalists: 2
- Imprisoned netizens: 31

Network condition

Connected to the web since the 1990s, the country began building infrastructure and relevant institutions in the mid-2000s. The founding of a National Steering Committee for Information and Communication Technologies and the 2005 launching of a national plan to develop TICs [3] have favoured Internet development.

Expansion of the network coincides with the blossoming of blogs and Internet cafés – as well as digital monitoring and control technologies.

The Communist Party of Vietnam has focused its ambitions on telecommunications, an industry which is proving dynamic. [4] The population of Internet users is booming: one in three persons is connected. And in Hanoi and Ho Chi Minh City, 95 per cent of people in the 15-22 age group have Internet access. [5]

The youthfulness of Vietnam's population and growing urbanization point to further explosive growth in Internet access.

Mediocre quality and speed

Despite these factors, the Vietnamese network has not achieved launch velocity. Its quality and speed lag behind those of other Asian countries. According to the 2012 Akamai report on the worldwide network, Vietnam's 1.25 Mbps average connection speed in the last quarter of 2012 ranks it below Thailand and Malaysia [6] and well below the international average of 2.3 Mbps.

Service providers at Party orders

Connection speed diminished since the beginning of last year. The reason is simple: the ruling party deliberately lowered the network's speed, by way of its control of Internet Service Providers.

Most of the country's 16 service providers are directly or indirectly controlled by the Party [7].The industry leader, Vietnam Posts and Telecommunications Group, which controls 74 per cent of the market, is state-owned. So is Viettel, an enterprise of the Vietnamese armed forces. FPT Telecom is a private firm, but is accountable to the Party and depends on the market leaders for bandwidth.

A distinction exists between service providers who enable individuals and companies to connect, and Internet Exchange Points (IXP), which allocate bandwidth to service providers.

Under Vietnamese law, service providers may be private firms, but IXPs are by definition state-owned [8]. Under this system, the government may control access to content, acting through its own companies, or through IXPs.

Monitoring systems

Service providers are the major instruments of control and surveillance. Providers block access to sites that displease the authorities. The procedure involves use of DNS (Domain Name Server), which enables access shutdown to a given domain name. But while DNS blocking affects access to an entire site, it cannot be directed at a specific page.

1 Whitebook „Viet Nam Information and Communication Technolology" – 2011. p.5 (http://mic.gov.vn/Attach%20file/sachtrang/sachtrang2011.pdf)

2 http://www.itu.int ; http://data.worldbank.org ; http://mic.gov.vn/

3 http://opennet.net/research/profiles/vietnam#footnoteref2_g3yqrfg

4 Ibid p.49

5 http://www.economist.com/blogs/banyan/2012/08/Internet-freedom-vietnam

6 http://english.vietnamnet.vn/en/science-technology/22586/Internet-speed-unimproved-owing-to-the-lack-of-content.html

7 http://english.mic.gov.vn/Statistics/staticstics_open/Trang/operators.aspx

8 http://www.business.gov.vn/assets/fbbc1d48c42d4f36a161a8a3d8749744.pdf art. 13.

Each service provider is allowed to block content individually, without having to do so jointly with the other firms. For example, VNPT censors Facebook, but the other providers allow access.

OpenNet Initiative, a research group, published a list in 2012 of sites blocked in Vietnam. These included newspapers and domestic and foreign blogs, and sites that provided content on political opposition and human rights.

Some bloggers have used circumvention software – proxies, VPN, Tor – to defeat blocking. But these tools are not always reliable. The government has the capability to block ports set aside for relaying encrypted data and making the attempted solutions unusable.

Bloggers monitored by the government frequently undergo *Man In The Middle* attacks. These are designed to intercept data meant to be sent to secure (https) sites. This technique can be used only by administrators of the Vietnamese network, for example Internet service providers. Frequently, passwords are hacked and connection speeds slowed down on days when dissidents are arrested or go on trial.

Subscription and personal data controls

Subscribers to landline service for telephone and Internet are required to submit a series of documents that contain personal data: name, date of birth, telephone number, job, employer and proof of address.

The sole proof of address officially recognized in Vietnam is the ***hộ khẩu***, a police document designed for population control. Without the ***hộ khẩu***, it is impossible to rent an apartment, obtain a formal job, receive a driver's license or subscribe to an Internet service. Three countries in the world use such a document: China, North Korea and Vietnam.

Mobile communications monitoring

The major Internet service providers also provide fixed and mobile phone service. Mobile phone service revenues reached an estimated $500 million in 2012 [1]. Vietnam had 119 million mobile service subscriptions – for a country of 91 million [2]. Three major mobile service firms, including Viettel [3], shared 90 per cent of this giant market. All are state-owned.

Freedom House reported in July 2012 that a survey showed that 91 per cent of respondents connected to the Internet on their mobile devices. But government ownership of the service providers means that security for mobile browsing is poor and surveillance easy

According to the report, the government monitors conversations and tracks the calls of citizens who are targeted as „activists" or „reactionaries". Some of them have had their telephone or Internet service cut off [4].

Official legal weapons

Vietnam's 1989 media law [5] explicitly defines the role of the press: *„The media operating within the Socialist Republic of Vietnam is the essential means of providing public information in relation to social life; is the mouth piece of Party organizations, State bodies and social organizations), and a forum for the people."*

The law creates boundaries on traditional and online media. Though freedom of the press, freedom of expression and the right to be informed are all guaranteed in Article 69 of the Vietnamese constitution of 1992, these freedoms are, in reality, discarded when they contradict the Party line.

In direct accord with the 1989 law, Decree 55/2001/ND-CP of August, 2001 sets out the basis for Party control of the Internet. Article 6 specifies that information posted on the Internet must meet media law standards. Article 8 declares that „the supervision of information on the Internet must be enforced by competent State agencies". Article 11 prohibits use of the Internet to oppose the government.

The decree also provides in Article 13 that IXPs (see above) can only be owned by the state.

1 Safety on the Line: Exposing the Myth of Mobile Communication Security, Freedom House, July 2012, p. 148, http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line.pdf

2 http://www.itu.int/ITU-D/ict/statistics/

3 http://mic.gov.vn/Attach%20file/sachtrang/sachtrang2011.pdf p.51

4 http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line%20vFINAL.pdf p.151

5 http://www.cov.gov.vn/cbqen/index.php?option=com_content&view=article&id=606&Itemid=75; http://www.unhcr.org/refworld/pdfid/50fe5e5a2.pdf

Another decree enacted in 2003, 92/2003/QD-BBCVT, prohibits sending or receiving anti-government material. The decree also requires site owners to register with the Vietnam Internet Network Information Center, an agency of the Ministry of Information and Communications. Since June 2006, Decree 56/06/ND-CP holds journalists and bloggers to Party discipline through a prohibition on *„expressing reactionary ideology or culture"* or *„spreading illegal propaganda"*, crimes punishable by 3 to 20 years in prison and a $2,000 fine.

Internet cafés, very popular in Vietnam, are strictly regulated. A decision by the Hanoi People's Committee in 2010[6] requires café owners to install government-supplied monitoring software that enables tracing of Internet activity as well as site-blocking. Under the decree, users connecting from cafés must show their identity cards, and the cafés are required to store this information, so that it can be officially inspected. According to our sources, café owners frequently ignore these requirements for economic reasons, because customers are known to quit patronizing an establishment that demands identification. Nevertheless, Internet cafés are required to keep all users' browser logs.

In April 2012, Reporters Without Borders called on the government to abandon a planned decree on „Management, Provision, Use of Internet Services and Information Content Online". With the announced aim of replacing a 2008 decree (itself an amended version of a 2001 decree), the proposed new law would:

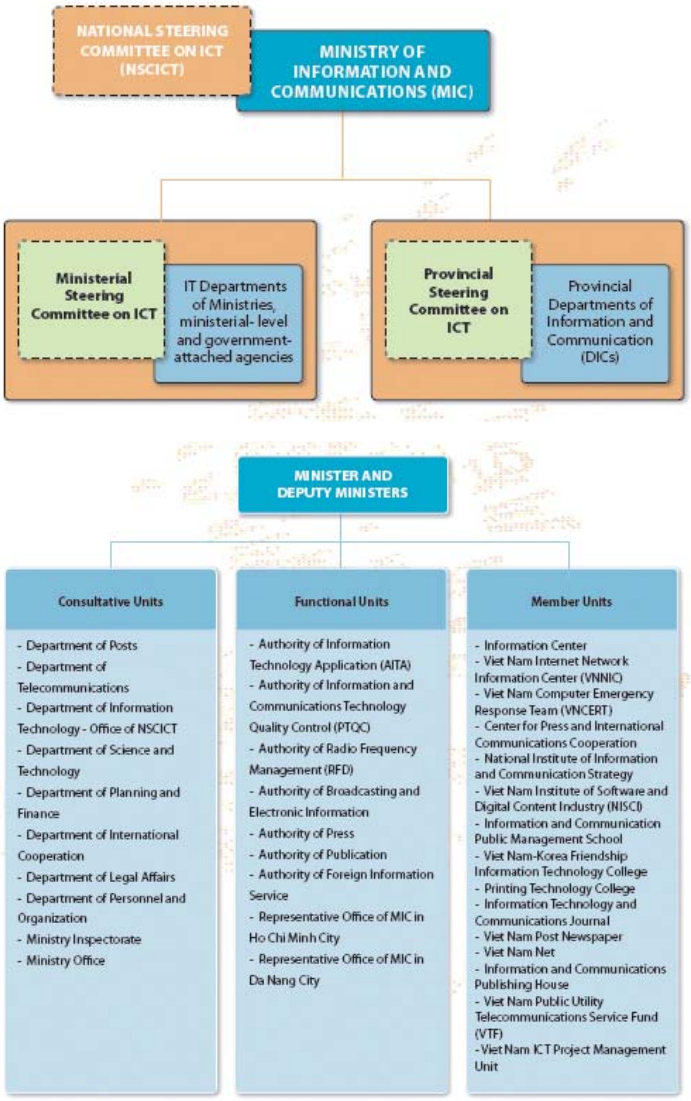
- Prohibit all anonymous online expression of opinion, and ban use of false identities or identity-masking tools.
- Prohibit false names on social networks.
- Require site administrators to report illegal activities to the government.
- Require bloggers to identify themselves by their real names – ending a practice by which they often use fictitious names in order to evade surveillance.
- Force foreign online providers to locate their data centres in Vietnam, thereby authorizing Party access.
- Require foreign providers to supply personal information on their users (name and address) and to cooperate with government agencies[7].

Control at the heart of institutions

Decisions concerning Internet monitoring originate mainly with the Ministry of Information and Communications and the Ministry of Public Security.

Ministry of Information and Communications

The MIC controls the major online service providers and the Vietnam Internet Network Information Center. In addition, the ministry issues most decrees involving Internet use. The ministry works close with the National Steering Committee for Information and Communication Technologies, which is headed by the prime minister[8].



Source : White Book 2011 Viet Nam Information and Communication Technology

6 http://www.fidh.org/IMG/pdf/bloggers_report_in_english.pdf p.9

7 http://english.vietnamnet.vn/en/science-technology/23242/new-Internet-draft-decree-favors-foreign-businesses.html

8 http://www.action.vn/news/hot-news/594-prime-minister-will-be-the-chairman-of-the-national-ict-committee

Ministry of Public Security

The ministry focuses on enforcing laws and sanctions that target publications deemed reactionary, by official standards, rather than on the technology of network monitoring.

However, the ministry runs the Công An Mạng digital police agency, which was founded initially to combat cybercrime, such as credit card fraud and hacking. But this force enjoys complete authority to shut sites or blogs that displease the government, and to arrest the authors. Lt. Col. Đinh Hữu Tân, chief of the „Internal Security Bureau" in Hanoi has said the force's job is to "monitor Internet content in all form, all publications, including press reports, blogs and commentaries [1].

Internet monitoring is openly acknowledged, but the size of the surveillance force and the details of the cyber-police's methods are kept secret.

Cyber-army

The Vietnamese web shows remarkable vitality, despite laws and institutions that impose Internet monitoring and censorship, as well as harsh repression against those exercising the right of free expression and the right to information.

Political and social blogs and dissident commentary are flourishing. Trying to contain them, the government has appealed to its own cyber-soldiers, who are dedicated to stamping out what are deemed anti-patriotic and reactionary opinions.

The cyber-army is not an official entity – though the authorities of Ho Chi Minh City have acknowledged deploying what they call „public opinion shapers". [2] Their identities are kept secret from the public, but they are believed to number more than 80,000 nationwide.

Following the Chinese model, this militia disseminates government propaganda and reports activists, bloggers and netizens to the government.

An estimated 1,000 cyber-officers [3] officially appointed by the government are assigned to infiltrate the favoured territory of information activists: social networks and blogs [4].

Major freedom of information violations

For the government, the blogosphere is the main target. Blogs represent an enormous new information and opinion sphere – one that arouses great interest by web users. For that reason, blogs are targeted for heavy sanctions.

Huynh Ngoc Chenh (Netizen of the year for 2013), sums up the situation: *„The state controls all communications. Opinions that oppose the state are not made public. Freedom of expression is practically non-existent in Vietnam. So many people use blogs to make their opinions known. But the government shuts these blogs. And many bloggers are arrested. And they are harassed, along with their families."*

In September 2012, Decree 7169/VPCP-NC directly targeted the country's most influential blogs [5]: Danlambao, Danglambao and Biendong. Their authors, who write under pseudonyms, face long prison terms if the Party discovers their real identities.

Anonymity is widespread in the Vietnamese blogosphere. But the Party is not letting that get in its way, using its monitoring tools to uncover the real names of targeted bloggers. If caught, they risk harsh punishment.

That was the fate of **Le Nguyen Sang and Huynh Nguyen Dao** in 2006. While both signed their work with false names (Nguyen Hai Son and Nguyen Hoang Long), they were identified by cyber-police and sentenced to four and two and a half years in prison, respectively.

Tran Huynh Duy Thuc was arrested in 2009, and **Lu Van Bay** in 2011, though both posted their work under pseudonyms. Thuc now is serving a 16-year sentence. Bay, who used four different false names, was sentenced to four years.

Blogger Panh Than Hai and writer **Pham Chi Dung**, a former member of the Ho Chi Minh City People's Committee who contributed to „unauthorized" sites such as Phiatruoc and Quanlambao were also arrested despite their use of false names.

1 http://www.fidh.org/IMG/pdf/bloggers_report_in_english.pdf p.10

2 http://www.france24.com/en/20130118-vietnams-propaganda-agents-battle-bloggers-online

3 http://techpresident.com/news/wegov/23377/vietnams-government-hired-propaganda-bloggers?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+techpres+%28techPresident%29

4 http://www.bbc.co.uk/news/world-asia-20982985

5 http://finance.yahoo.com/news/under-fire-vietnamese-blogger-vows-dissent-093346513.html

Information activists live under constant monitoring. Methods include physical surveillance and intimidation [6] of those whose identities are known. Phishing and digital espionage is directed at anonymous bloggers.

One activist, who had served a prison sentence and asked to remain anonymous, told Reporters Without Borders said that following his arrest: *„In prison they showed me the articles I had written, signed with a false name, the emails I had sent to colleagues and even my telephone conversations."*

This is not an isolated case. Cyber-police use all possible methods, including Man In The Middle password retrieval, hacking attacks, and mobile phone monitoring. The police aim not only to uncover bloggers' real names, but to identify everyone in their networks.

The official justification in all of these cases is always *„cooperation with reactionary organizations based abroad", „attempt to overthrow the government", or „anti-government propaganda"*.

Corruption and tax fraud allegations are also frequently aimed at journalists and bloggers. Dieu Cay, a well-known and popular blogger, was sentenced to 10 years in prison in on these charges in 2008.

The repression campaign targets individual as well as collective blogs. In the former group are bloggers including Nguyen Van Dai, Pham Thanh Nghien, Le Cong Dinh, Dinh Dang Dinh, J.B Nguyen Huu Vinh, Nguoi Buon Gio, and Nguyen Quang Lap. Collective blog targets include BachDang, Quanlambao, Bauxite Viet Nam, Dong Chua Cuu The, and Nu Vuong Cong Ly.

The list is steadily growing longer. On 9 January 2013, 14 activists, including 8 bloggers and netizens were sentenced to terms ranging from 3 to 13 years in prison – a collective total of 113 years behind bars. They were charged under clauses 1 and 2 of Article 79 of the Penal Code with *„participation in an attempt to overthrow the people's administration" and „organization of an attempt to overthrow the people's administration"*.

Constant monitoring creates pressure for self-censorship by activists whose families come under official pressure. Yet despite everything, the Vietnamese web remains enormously active. For one thing, the Party does not have the capability to monitor the entire web. And authorities cannot new blogs from springing up.

Some bloggers use anti-monitoring tools, such as proxies, in order to keep up their activities. And many are defiantly posting under their real names, or publicly denouncing the official campaign against them. In the words of an administrator of Danlambao: „Nobody can shut our mouth or stop our freedom of expression. This is our mission, we will continue at any cost. [7]"

Technical solutions

In order to protect their anonymity in a country where the network infrastructure does not allow interception of encrypted communications (meaning no Deep Packet Inspection), Vietnamese bloggers have every reason to use encryption. Consequently, VPN is a better option than proxies. The latter enable bypassing of access blockage, but – unlike VPN – do not encrypt.

Temporary or disposable email services are a good way to preserve anonymity. Use of anonymous and secure email services such as Riseup.net or hushmail, coupled with PGP encryption, can also be useful.

Telephone or VOIP conversations should be avoided. Vietnamese surveillance is also physical. One of the methods used to intercept these conversations is to use a long-range microphone in the vicinity of a suspected activist's home.

Use of instant messaging services, such as Google chat, ICQ, IRC, or Yahoo!, coupled with encryption software such as OTR, can defeat this kind of surveillance. A great advantage of OTR is that no trace of the message history remains on a user's device.

For more information, read our Online digital kit

6 http://en.rsf.org/vietnam-arrests-surveillance-and-18-07-2012,43061.html

6 http://finance.yahoo.com/news/under-fire-vietnamese-blogger-vows-dissent-093346513.html

CYBER-CENSORSHIP IN 2012 – AN OVERVIEW

Key events in Internet censorship and surveillance in 2012 and first two months of 2013

INTERNET GOVERNANCE AND NET NEUTRALITY

UN Recognition of the right to freedom of expression on the Internet

The United Nations Human Rights Council affirmed the right to freedom of expression on the Internet for the first time in a resolution on 5 July 2012, taking the position that „the same rights that people have offline must also be protected online (...) regardless of frontiers and through any media." The resolution called on all countries „to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries."

World Conference on International Telecommunications (WCIT)

Different visions of Internet governance and, indirectly, the future of online news and information competed and clashed at the World Conference on International Telecommunications, which the International Telecommunication Union (ITU) staged in Dubai in December 2012. At the end of the conference, fewer than half of the ITU's member countries (89 out of 193) signed a new treaty revising the International Telecommunications Regulations (ITR). A coalition of 55 countries, including the United States and European Union countries, refused to sign it on the grounds that some of its provisions on spam management and Internet security, and a separate text that was adopted in a chaotic manner, Internet Resolution PLEN/3, would be used by countries that traditionally control the Internet to justify their censorship, filtering and blocking. The lack of civil society participation and procedural transparency was strongly criticized by many NGOs, with support from UN Special Rapporteur for Freedom of Expression and Opinion Frank La Rue.

The Dubai summit should have been used to defend the Internet as a place of freedom, as a place for the free exchange of views and information. But instead it highlighted the fight between different countries for influence over the Internet. More information: Centre for Technology and Democracy and an analysis of the new ITR by Access.

EU rejects Anti-Counterfeiting Trade Agreement

On 4 July 2012, the European Parliament rejected the Anti-Counterfeiting Trade Agreement (ACTA), which threatened fundamental online freedoms including access, freedom of information, Net Neutrality, innovation, and the sharing of free technology. Its rejection was a victory for citizen campaigning, which was mobilized by advocacy groups such as La Quadrature du Net and Panoptikon.

Netherlands and Slovenia back Net Neutrality [1], Brazil drags its feet

In December 2012, Slovenia followed Netherlands and Chile in adopting a law that enshrines Net Neutrality and prohibits Internet Service Providers from discriminating against any kind of online traffic.

But adoption of a proposed Internet „Civil Framework" law continues to be postponed in Brazil because of pressure from the film and music industries. Widely supported by Brazilian civil society, which regards it as a model law, the so-called „Marco Civil" would define the rights and responsibilities of the state, Internet Service Providers (and other technical intermediaries) and Internet users as regards Internet usage, copyright and personal data protection, while safeguarding Net Neutrality, privacy and the free flow of information online.

1 See glossary

Filtering violates fundamental rights

In a decision against Turkey on 18 December 2012, the European Court of Human Rights ruled for the first time that blocking a website violated article 10 (on freedom of expression) of the European Convention on Human Rights.

The Strasbourg-based court said: „The Internet has now become one of the main means for individuals to exercise their right to freedom of expression and information; it offers essential tools for participating in activities and debates on political matters and issues of public interest."

The Court of Justice of the European Union already ruled on 24 November 2011 that generalized content filtering violates fundamental rights.

Internet companies stress transparency

The latest issue of Google's „Transparency Report", released in November 2012, points to a big increase in government surveillance. Google said government requests for user data had risen steadily since the publication of its first Transparency Report. In June 2012, Google voiced concern about an increase in requests for the removal of pages with political content. The country by country evolution of user data requests can be seen here and removal requests can be seen here.

Google's transparency initiative has been adopted by others. Twitter launched its own transparency report in July 2012. It focuses on user data requests by governments (the United States made the most requests) and on content removal requests by governments or copyright holders. Twitter has also undertaken to leave a „Tweet withheld" message whenever a Tweet is removed in response to a complaint from a copyright holder and to send a copy of each takedown notice to the Chilling Effects website.

LEGISLATIVE OFFENSIVES

More surveillance to ensure cyber-security?

Repressive legislative initiatives by authoritarian regimes have been compounded by parallel initiatives in countries that claim to be democratic and to respect individual freedoms. The latter are all the more disturbing as they provide authoritarian regimes with justification for their own initiatives.

Britain

The British Communications Data Bill will have to be revised after Deputy Prime Minister Nick Clegg announced in December 2012 that he would block it. The version of the bill that was published in the spring of 2012 would give the police and intelligence services extensive access to phone records, emails and Internet browsing history on the grounds of the need to combat terrorism and other serious crimes.

United States

Opponents of the proposed Cyber Intelligence Sharing and Protection Act of 2011 (CISPA) say it will allow privacy to be violated in order to protect cyber-security. Although it seemed to have broad support in the US Congress, it caused such an outcry that substantial revisions were made to increase protection for privacy, the White House threatened a veto and a sizeable number of representatives ended up voting against it. A new version of CISPA was resubmitted in January 2013 and could come before Congress as early as April 2013.

Netherlands

Claiming that anonymization tools such as Tor are hampering the work of tracking down cyber-criminals and pedophiles, the Dutch government has been pressuring legislators to pass a law that will reinforce police cyber-surveillance powers regardless of whether the target computer is located in the Netherlands or abroad. The proposed law would allow the police to remotely search computers, install spyware and delete illegal content without having to submit a legal assistance request to the country concerned if the target computer is located abroad. Read the Electronic Frontier Foundation analysis.

Philippines

The supreme court of the Philippines voted unanimously on 9 October 2012 to stay implementation of the Cyber-crime Prevention Act 2012 (Republic Act No, 10175) after receiving more than a dozen petitions asking it to rule on the law's constitutionality. Reporters Without Borders calls for its repeal because its attempt to combat cyber-crime poses a major threat to freedom of information. Online defamation was added to the law's list of „cyber-crimes" at the last minute, before adoption.

Malawi

The Media Institute of Southern Africa (MISA) has criticized a government attempt to regulate and control online publications in the form of a so-called E-Bill that would force online publication editors to publish their names, addresses and phone numbers and would create a cyber-police with the job of monitoring the Internet for illegal activity.

Peru

A proposed cyber-crime law is likely to restrict online freedom. On the initiative of the NGO Access, university academics and civil society representatives have written an open letter to parliament criticizing the bill.

Iraq

In January 2012, the Iraqi parliament repealed a cyber-crime law that was criticized for its overly broad definition of the crimes it intended to punish (for example, "violating religious, moral and social principles") and for draconian penalties that included life imprisonment for using a computer to besmirch the country's reputation. Read the Access Now analysis.

Protecting minors, the perfect pretext

Russia

In the name of „protecting minors", a federal government agency began on 1 November 2012 to compile a blacklist of „harmful" websites liable to be blocked without reference to a court and without any right of defence. The vague and broad definition of the targeted content (pornography, extremism, defending suicide, encouraging drug use and so on) and the supervisory body's lack of independence open the way to overblocking. Age category labelling – "banned for minors under the age of" 6, 12, 16 or 18 – was also imposed on all news websites. A bill banning online censorship circumvention tools has also been submitted to a Duma committee.

Canada

Draft Federal Law C-30, also known as the Protecting Children from Internet Predators Act, which the public safety ministry submitted to parliament on 14 February 2012, would place Internet users under close surveillance. It would allow the police to request phone records without first seeking a court warrant. Internet Service Providers and mobile phone operators could be forced to install surveillance devices and record subscribers' communications. The police could also, without a court warrant, install a device that could capture the IP address of any device connected to the Internet.

Copyright v. online freedom of expression

United States

The proposed „Stop Online Piracy Act" (SOPA) and «Protect IP Act» (PIPA) elicited a great deal of domestic and international criticism of the danger of unprecedented Internet censorship. Their opponents said they would prejudice countless Internet users who had never violated intellectual property by forcing websites to block access to other sites accused of vaguely defined copyright violations. The bills were finally shelved, but for how long?

Panama

In September 2012, parliament passed Law 510, which restricts freedom of expression and access to online information and creates a General Directorate for Copyright with the task of tracking down violators and imposing heavy fines on them without reference to a court. NGOs and civil society representatives wrote an open letter to President Ricardo Martinelli urging him not to sign what they called the „worst copyright protection law in history". Read comments by netizens on Global Voices.

Other disturbing legislation

In Malaysia, an amendment to the 1950 Evidence Act makes Internet service operators automatically liable for any posted content or content transiting through their services that is deemed to be defamatory. Owners and managers of Internet cafés and blog platforms are among those affected by this presumption of guilt. The Centre for Independent Journalism organized an online protest against the amendment.

ALL-OUT FILTERING

International filtering

Censorship of the anti-Islamic video „Innocence of Muslims" inflicted major collateral damage on access to online information. The filtering and blocking measures ordered in many countries often resulted in suspension of access to YouTube and in some cases, all communications. Whether as a result of court or administrative decisions, the video has probably been blocked in more countries than almost any other piece of online content ever. The countries that blocked it include Saudi Arabia, Afghanistan, Pakistan, Bangladesh, Egypt, Turkey, Russia, Kazakhstan, Kyrgyzstan, India and Bahrain.

China – race against the clock

China's censors had their hands full in recent months trying to block the online dissemination of sensitive stories, including:

- The New York Times story on Wen Jiaobo's fortune
- Opposition to censorship of a New Year editorial in the newspaper Nanfang Zhoumo that called for constitutional reforms in China
- The many cases of self-immolation in Tibet
- Corruption
- Criticism of the government's handling of flooding in the summer of 2012.

Censorship was intensified in the run-up to the Communist Party Congress that appointed a new generation of rulers and put Xi Jinping in charge.

Massive Internet censorship in Tajikistan

In 2012, there were several waves of blocking of leading news websites such as Asia Plus, RIA-Novosti, Lenta.ru, Fergananews.com, Centrasia.ru, and the BBC, as well as YouTube and Facebook. The National Telecommunications Agency is now in the habit of issuing orders to Internet Service Providers to block access to any sensitive content such as news analyses questioning the government's stability, reports of armed clashes or criticism of the president on social networks.

Mass blocking in Kazakhstan

Sham legal proceedings were used in December 2012 to ban Kazakhstan's leading opposition media on the grounds of alleged „extremism". This resulted in the blocking of all websites carrying the online versions of the newspaper *Vzglyad* and the *Respublika* network of newspapers, as well as their social network accounts. The online TV station *K+* and the news portal *Stan.tv* were also blocked.

In India, censorship to suppress rumours?
In an attempt to halt violent inter-ethnic unrest, the Indian authorities ordered Internet Service Providers to block access to more than 300 pieces of online content in August 2012. Some did encourage violence by relaying baseless rumours, but others, such as content on the websites of *AFP, Al-Jazeera* and the Australian TV station ABC, just consisted of straightforward news photos or news stories. See the list of blocked content published by the Centre for Internet and Society.

Pakistani electronic Great Wall – fact or fiction?
Plans for a national Internet filtering and blocking system intended to block access to millions of „undesirable" websites using Deep Packet Inspection (DPI) were revealed in early 2012. The Daily Times reported that the National ICT Research and Development Fund, an offshoot of the information technology ministry, issued an invitation to submit bids for the creation of the system, expected to cost 10 million dollars, and that several international companies responded. A petition was launched urging companies not to respond. Statements by officials opposing the project were subsequently reported by the media. Pakistan civil society *remains vigilant*.

RESTRICTED ACCESS?

Two billion people worldwide now have Internet access but, for a third of them, access is limited by government censorship, filtering and surveillance. Infrastructural development problems and purely political considerations sometimes limit expansion of access.

National Internet in Iran
In September 2012, the government accelerated the creation of a national Internet with a high connection speed but entirely monitored and censored. The grounds cited for speeding up implementation was a wave of cyber-attacks on Iran's nuclear installations. All Iranian websites are eventually supposed to be hosted on local servers. Applications and services such as email, search engines and social networks are to be developed under government control. So far only government offices are connected to this national Internet, but it is feared that eventually all Iranian citizens will have no choice but to follow suit. (See the Iran chapter of „State enemies".)

Frequent Internet cuts in Syria
Internet and telephone are often deliberately cut in targeted locations, in addition to cuts due to power blackouts. Syria was completely disconnected from the Internet for about two days at the end of November 2012, at a time when the regime was accused of planning a nationwide massacre.

High-speed fibre-optic broadband finally in Cuba?
Completed in 2011, the submarine fibre-optic broadband cable from Venezuela to Cuba was finally put into service in August 2012, the network specialist company Renesys reports. But Global Voices quoted the government daily *Granma* as saying that, although the test phase has been completed, Cubans should not expect a dramatic increase in the availability of Internet access in the short term. Until then, Cuba was using very limited satellite connections to access the international Internet (see the Cuban chapter of the 2012 Enemies of the Internet report).

Regional discrimination
Suspension of Internet access and telecommunications are common in Tibet and Xinjiang during periods of crisis (see the China chapter of the 2012 Enemies of the Internet report).

At the behest of the government of India's northern state of Jammu and Kashmir, telephone operators suspended service in the Kashmir Valley last August, on the anniversary of India's independence, which is always a sensitive time.

In Pakistan, mobile phone networks were temporarily disconnected in the southwestern province of Balochistan on the anniversary of the country's independence in August 2012.

NETIZENS TARGETED

Tributes

A total of 47 netizens and citizen-journalists were killed in 2012, most of them in Syria. They act as reporters, photographers and video-cameramen, documenting their daily lives and the government's violent crackdown. Without them, the Syrian government would be able to impose a complete news blackout in some regions and carry out massacres undetected.

In Iran, the blogger Sattar Beheshti died in unknown circumstances following his arrest on 31 October 2012. The available information suggests that he died from blows received during interrogation. No one has been arrested for his death.

In Bangladesh, the blogger Ahmed Rajib Haider was hacked to death near his home in the capital, Dhaka, on 15 February 2013.

In Pakistan, the 14-year-old blogger **Malala Yousufzai** only narrowly survived being shot in the head by Taliban gunmen on 9 October 2012.

Mass arrests

About 180 netizens are currently detained in connection with their provision of news and information. The world's five biggest prisons for netizens are China (with 69 detained), Oman (32), Vietnam (31), Iran (20) and Syria (18).

Mass arrests and raids on news outlets have taken place not only in Syria but also in the Sultanate of Oman and in Iran, on „Black Sunday". In Sri Lanka, nine employees of the online newspaper Sri Lanka Mirror were arrested in a raid in July 2012.

Vietnam continues to arrest netizens and give them long prison sentences. The well-known blogger Dieu Cay got 12 years. In China, Tibetan monks are jailed for trying to inform the outside world about the many cases of self-immolation. Azerbaijan goes after bloggers who stray from the official line.

The conditions in which netizens are imprisoned are often appalling and mistreatment is frequent. Some detainees, especially in Iran, are denied the medical treatment they need and risk dying in detention.

Threats and violence

Nineteen bloggers were openly threatened on Islamist websites and at demonstrations in Bangladesh in February 2013 in connection with the trial of several former leaders of Islamist parties including Jaamat-e-Islami on war crimes charges.

The „Courage for Tamaulipas" Facebook page, which covers organized crime violence in the Mexican state of Tamaulipas, angered drug traffickers, who are offering 600,000 pesos ($46,000) to anyone who could identify the page's editor or the editor's family.

Ruy Salgado, a Mexican blogger who ran El Santuario, a website famous for its coverage of corruption, gave up his online activities because of the threats he was getting.

The families of netizens, especially those who are detained, are often subject to harassment, pressure and threats. This is the case in Iran, especially for the families of Iranian journalists and bloggers who are based abroad, and in Vietnam.

Imprisoned Vietnamese blogger Ta Phong Tan, the creator of the „Justice and Truth" blog, suffered a additional blow last July when her mother took her own life by setting herself on fire outside the headquarters of the People's Committee in Bac Lieu, Tan's home province, in an act of despair about the way Tan was being treated. Tan is now serving a 10-year jail sentence.

Trial of WikiLeaks source Bradley Manning

US Army Private Bradley Manning confessed before a court martial on 28 February 2013 that he passed military and diplomatic files to WikiLeaks, including US embassy cables, the files of Guantanamo detainees and videos of air strikes in which civilians were killed, in particular the „Collateral Murder" video that showed a US helicopter crew killing *Reuters* journalists.

He said his motive was to enlighten the public about what goes on and to „spark a debate about foreign policy". He explained that he initially tried to give the files to the *New York Times* and *Washington Post* but could not find anyone who seemed interested. He also claimed that he chose the material with care in order to ensure that it would not cause any harm.

Manning is facing up to 20 years in prison. Many NGOs have criticized the conditions in which he was being held as humiliating.

DataCell, a company that collected donations for WikiLeaks, meanwhile complained to the European Commission about Visa Europe, MasterCard Europe and American Express after they stopped processing donations for WikiLeaks in December 2010. In a preliminary decision in November 2012, the commission said a block on processing donations for his organisation by credit card companies was unlikely to have violated EU anti-trust rules.

NETIZENS FIGHT BACK

In the face of offensives by governments and interests groups seeking to control the Internet, netizens and online news providers have sought to organize, campaign and resist with varying degrees of success.

The most noteworthy initiatives of recent months include:

- The phenomenon of Internet memes, content that passes rapidly from person to person online, going „viral" and often evolving in the process, in a form of spontaneous online popular culture. They typically use humour and Photoshop editing to make fun of social or political issues and, in countries such as China, to evade filtering by censors. Chinese examples include Grass Mud Horse, which uses wordplay in a popular song to mock censorship, and the artist Ai Weiwei's sunflower seeds.
- The online resistance to censorship of the Chinese newspaper Nanfang Zhoumo's New Year editorial calling for constitutional reforms.
- The role played by WCITLeaks in promoting transparency during the negotiations over a new International Telecommunication Union treaty at the World Conference on International Telecommunications in Dubai in December 2012.
- The campaign by the French advocacy group La Quadrature du Net against the Anti-Counterfeiting Trade Agreement (ACTA).
- The first Stop Cyber Spying campaign, a week of online protest in the United States against the proposed Cyber Intelligence Sharing and Protection Act of 2011 (CISPA), and the new Stop Cyber Spying campaign in response to the proposed Cybersecurity Act of 2012 (CSA).
- The Save Your Voice campaign by civil society and Internet users in India to demand repeal of the IT Rules, legislation that limits online freedom of expression. Two cyber-activists even went on hunger strike.
- The blackout of 500 websites in Jordan on 29 August 2012 to protest (#BlackoutJO and #FreeNetJO) against repressive amendments to the press and publications law.
- The Stop Online Spying campaign that the Canadian advocacy group Open Media launched last September with a petition against the C-30 bill.
- The campaign for Internet freedom in Azerbaijan waged by the ExpressionOnline coalition and other groups during the Internet Governance Forum in Baku in November 2012.

Send us information about the campaigns to defend online freedom of expression and information that have impressed you most.

REPORTERS
WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

INTERNATIONAL SECRETARIAT REPORTERS WITHOUT BORDERS

47 rue Vivienne, 75002 Paris, France - Tel : 33 1 4483-8484 - Fax : 33 1 4523-1151 - Website : www.rsf.org - E-mail : rsf@rsf.org - Ambroise Pierre - Africa desk : afrique@rsf.org - Benoît Hervieu - Americas desk : ameriques@rsf.org - Benjamin Ismaïl - Asia desk : asie@rsf.org - Johann Bihr - Europe desk : europe@rsf.org - Soazig Dollet - Middle East desk : moyen-orient@rsf.org - Lucie Morillon - Internet desk : internet@rsf.org - Press contact : presse@rsf.org

REPORTERS WITHOUT BORDERS promotes and defends the freedom to be informed and to inform others throughout the world. Based in Paris, it has eleven international offices (Berlin, Brussels, Geneva, Madrid, New York, Stockholm, Tripoli, Tunis, Vienna and Washington DC) and more than 150 correspondents in all five continents.

Editorial Team: Grégoire Pouget, Hauke Gierow, Reza Moini, Benjamin Ismail, Pierre Belmont, Soazig Dollet, Benoît Hervieu, Johann Bihr, Ambroise Pierre, Antoine Héry, Olivier Basille | Chief Editor: Lucie Morillon