CAUSE

A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation

Coalition Against Unlawful Surveillance Exports

AMNESTY INTERNATIONAL

DIGITALE GESELLSCHAFT

fidh

HUMAN RIGHTS WATCH

OPEN TECHNOLOGY INSTITUTE

PRIVACY INTERNATIONAL

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

access

This report is published by the Steering Committee of the Coalition Against Unlawful Surveillance Exports (CAUSE). CAUSE was formed in April 2014, and brings together internationally focused NGOs and activists to initiate a global call for action from national governments and regional institutions, as well as raising awareness about the privatised surveillance industry and the damaging impact surveillance technologies have on human rights.

Contents

Introduction

The need to regulate the transfer of surveillance technologies that pose a risk to human rights has been largely recognised by EU institutions and some EU member states. It is no longer a question of if the EU should do more in this area, but how.

Since 2011, Regulation No. 428/2009, regulating the European export of dual-use items, has been under review by the European Commission, which is expected to produce a new draft Regulation by the end of 2015. This is a critical opportunity to ensure that surveillance technologies are properly and effectively brought within the purview of European dual-use export control policy.

It is not enough for EU member states to recognise the imperative of bringing surveillance technologies within the Dual Use Regulation. The Regulation must be sufficiently comprehensive, detailed and precise to ensure that all relevant technologies are regulated, while preserving a space for security research and the development of ICTs essential to the realisation of human rights. For export control policy to be effective in stemming human rights violations, the Regulation must require the consideration of human rights implications by export control authorities. Finally, the Regulation must address disparate national policies facilitating licencing avoidance and potential loopholes in enforcement mechanisms.

Translating in-principle commitments to stopping the flow of surveillance technologies to governments and agencies with troubling human rights records, into effective and accurate policy will require the prioritisation of these factors. The Coalition Against Unlawful Surveillance Exports (CAUSE) calls on European member states and the Commission to ensure that the draft Regulation reflects these concerns.

This briefing, and in particular the recommendations contained herein, are designed to guide the Commission in its review of the Dual-Use Regulation in 2015, in advance of the expected publication of a draft Regulation in early 2016.

Amnesty International
Digitale Gesellschaft
FIDH
Human Rights Watch
Open Technology Institute
Privacy International
Reporters Without Borders
Access

June 2015

The surveillance industry in numbers

182

Number of companies working in the EU

$ 5,000,000,000

Value of industry **5 billion** dollars

100 TRILLION

Emails that can be kept on one retention server

15

No. of companies that sell intrusion software

100,000 VOICE CHANNELS

Can be targetted by the VASTech Zebra System

Distance Cobham's IMSI Catcher can operate at in urban settings

40 ANTI-VIRUS APPS

Intrusion software regularly tested against to avoid detection

€ 139,000

Cost of basic FinFisher software, as quoted by Dreamlab and then marketed to Turkmenistan

€ 65,000,0000

Sales of Amesys' Eagle system in 2011

30-40 MILLIONS OF MINUTES

Recorded every month by Gaddafi with VASTech's Zebra system

100,000

Selectors available in the ETI-AS' system

Recommendations

The review of the Dual Use Regulation must ensure that:

All relevant surveillance technology is subject to licensing.

- The EU should review and establish an autonomous list of equipment and technology used for surveillance, reviewed on a regular basis, and subsequently seek to introduce the categories into the Wassenaar Arrangement ("WA").[1]
- The use of a dedicated catch-all mechanism, with stipulation on end-use and end-users, should be employed to future proof the Dual-Use Regulation in light of technological developments by allowing member state authorities to subject emerging technologies of concern to export authorisation.
- Items that should be subject to licensing are those specially designed and marketed for use in intelligence gathering and law enforcement by governmental agencies.
- Protections for security research and open source software need to be explicit to ensure security researchers are not unduly impacted.
- Regulatory changes aimed at increasing the effectiveness of enforcement of Intangible Technology Transfers must not inhibit legitimate security research.
- Security researchers, industry, and civil society must be involved in policy formulations and definitions and have the opportunity to assess and influence any controls on surveillance technology.
- Surveillance technologies should be included in EU embargoes on equipment that might be used for internal repression.

Human rights implications are appropriately incorporated within assessment criteria, consistent with obligations under the Charter of Fundamental Rights of the European Union.

- The Regulation should adopt a human rights, rather than "human security" approach to export controls, consistent with obligations under the Charter of Fundamental Rights of the European Union.
- Assessment criteria should also take into consideration
  - the human rights record of the end user of the technology;
  - the potential for the technology to be used in an unlawful manner, that is a manner not compliant with international human rights standards;
  - the weakness or absence of an appropriate legal framework to regulate the use of the technology by the end user.
- Governments must exercise a policy of restraint, and act on a presumption of denial for export license applications of surveillance technology.
- EU member states should use the eight common criteria for arms exports (EU Common Position)[2] to assess applications for surveillance technologies.
- An annual forum should be established for external experts and civil society to submit evidence and concerns on the content and scope of the EU Control List.

[1] Wassenaar Arrangement, "Best Practices For Implementing Intangible Transfer of Technology Controls (Agreed at the 2006 Plenary," available at http://www.wassenaar.org/guidelines/docs/ITT_Best_Practices_for_public_statement.pdf

[2] European Union External Action, "Arms Export Control," available at http://www.eeas.europa.eu/non-proliferation-and-disarmament/arms-export-control/index_en.htm

Disparate national policies facilitating licensing avoidance and potential loopholes in enforcement mechanisms are addressed, and greater transparency of exports is promoted.

- There needs to be capacity building between licensing authorities in the EU to ensure accurate information sharing and a consistent understanding of the technologies and risks in question.
- The expansion of brokering controls to include surveillance technologies should be examined.
- Member states should submit to the Council of the EU data concerning applications for licenses of surveillance technology, which should subsequently be made publicly available. The data should contain the category of licence applied for, the category of equipment applied for, details concerning the exporter, details concerning the end-user, the total cost of the license applied for, the destination of the export for which the license has been applied for, and the decision by the licensing authority concerning the application.
- Member states should share and publicly disclose approved licenses and transfers of surveillance technologies and the list of companies supplying surveillance technologies.
- Review processes should be established allowing for civil society expertise to be included at both national and EU levels.
- Policies and procedures should be adopted to stop or address misuse of products and services including contractual provisions that designate end use and end users, the violation of which would allow the company to withdraw services or cease technical support or upgrades.

Security research and the development of IT security tools are not subject to controls and are subject to explicit exemptions.

- The Regulation should ensure that controls on surveillance technology are constructed in a narrow and targeted manner such that legitimate security research and the development of legitimate security tools do not fall under the purview of controls, and that research activities are not chilled through ambiguous language.
- Implementation Guidance notes should be developed to accompany the Regulation, and should:
  - Clarify to what extent legitimate security research is protected by the general exemptions.
  - Explicitly state that specific legitimate security research, such as private exploitation research, and legitimate security items such as anti-virus products, fuzzers, defensive pentesting, exploit generation software and jailbreak software, are not caught by the Regulation.
  - Ensure that any items subject to licensing are only those specially designed and marketed for use in intelligence gathering and law enforcement by or for governmental agencies.
  - Encourage government to consult with industry and civil society to promote implementation of "know your customer" policies that will reduce the potential for approved, or otherwise permissible, exports to misappropriated for the abuse of human rights.

Controls of encryption and encryption products should be eradicated.

- EU member states and the External Action Service should actively push for further de-control of cryptographic items internationally, particularly within the Wassenaar Arrangement.

Background to the review of the Dual-Use Regulation

Particularly since the Arab Spring, civil society, the European Parliament, and some EU member states have been calling for the EU to introduce trade controls on ICTs that pose a risk to human rights in third countries. Some surveillance technology is already subject to export licensing across the EU because it falls within Annex 1 of the EU Dual Use Regulation (428/2009), while expedited 'general licenses' also contain clauses aimed at stopping transfers of surveillance technology where they pose a risk to human rights. The EU has also included some surveillance technology as part of its restrictive measures on Iran and elsewhere, and some member states can use ad-hoc measures such as the 'catch-all clause' within the Dual Use Regulation to restrict specific transfers, as Italy did in 2012 to control the sale of surveillance technology to Syria.

Since 2011, the EU has been conducting a review of the Dual Use Regulation.[3] The explicit aim of the review, mandated by the Regulation itself, is to ensure that security objectives are adequately met by export controls while European industry is not overly and disproportionately burdened. In 2011, the European Commission published a Green Paper[4] and call for evidence, followed by a report on the public consultation being adopted in January 2013.[5] Regarding surveillance technology, the Commission Communication published in 2014[6] recognised the risk posed by "the emergence of specific 'cybertools' for mass surveillance, monitoring, tracking and interception," while importantly also recognising "the interlinkages between human rights, peace and security."

Any changes to the Regulation will need to be agreed upon by all member states, as well as by the European Parliament. The Parliamentary Subcommittee on Human Rights and the Committee on International Trade convened a hearing in January 2015. In April 2015, the Foreign Affairs Committee of the European Parliament adopted a report by MEP Marietje Schaake on Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries. The report will be voted on by the plenary in summer 2015.

The Commission has also initiated an impact assessment aimed at informing the policy-making process by quantifying and providing objective data on the industry and the potential cost of any regulatory changes. Ecorys, a European research and consultancy company,[7] in partnership with the Stockholm International Peace Research Institute (SIPRI), is carrying out a data collection project, including a component specifically focused on surveillance technologies, to inform the impact assessment. The impact assessment is expected to be completed in the second half of 2015.

Simultaneously, a Subcommittee on ICTs, the Surveillance Technology Working Group (STEG) has been established within the DG Trade Dual Use Working Group. Consisting of experts from the national licensing authorities in Germany, the Netherlands, Finland, Sweden, Denmark, the UK, France and Poland, the working group is aimed at identifying surveillance technology that poses a risk to human rights and how it can be effectively controlled.

[3] European Commission Roadmap: Review of the EU dual-use export control regime (15 July 2014), available at http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_trade_014_dual_use_en.pdf

[4] European Commission, "Green Paper: The dual-use export control system of the European Union: ensuring security and competitiveness in a changing world," (30 June 2011), available at http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf

[5] European Commission, "Commission Staff Working Document: Strategic export controls: ensuring security and competitiveness in a changing world – A report on the public consultation launched under the Green Paper COM (2011) 393," (17 January 2013), available at http://trade.ec.europa.eu/doclib/docs/2013/february/tradoc_150459.pdf

[6] European Commission, "Communication from the Commission to the Council and the European Parliament: The Review of export control police: ensuring security and competitiveness in a changing world," (24 April 2014), available at http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf

[7] http:// http://www.ecorys.com

Surveillance technologies and human rights

The human rights impacts of surveillance exports are becoming increasingly evident: the private text messages of activists are read out to them as they are tortured; mass surveillance technology appears on the market, for purchase by repressive regimes that wish to monitor, collect and store the communications of entire populations; political refugees find their computers have been hacked and their digital life stolen. Surveillance technologies are used by governments to target opponents, journalists and lawyers, crack down on dissent, harass human rights defenders, intimidate populations, discourage whistle-blowers, chill expression and destroy the possibility of private life. In some cases, they also used to subject entire populations to indiscriminate monitoring. In short, they are often part of a broader state apparatus of oppression, facilitating a wide variety of human rights violations including unlawful interrogation practices, torture and extrajudicial executions.

The most obvious right affected by surveillance technology is the right to privacy, as any interception with communications or collection of personal data constitutes an interference with the right to privacy. Other rights that are frequently directly affected by surveillance include the right to freedom of expression and the right to freedom of association.

The unlawful surveillance of communications and their interception has been recognised by the European Council as a violation of the right to privacy and can lead to restrictions on other freedoms including expression, association and political participation as well as further human rights violations including arbitrary arrest and detention, torture and other cruel, inhuman or degrading treatment or punishment. The export of European made surveillance technologies to countries where they are likely to be used in an unlawful manner, that is in a manner not compliant with human rights standards, should be urgently addressed. The consideration of the lawfulness of any acquisition of surveillance technologies should encompass consideration of the weakness or absence of an appropriate legal framework in the recipient country regulating the use of the technology in compliance with international legal standards, including in particular the European Convention on Human Rights.

Furthermore, it should be reiterated that EU member states' human rights obligations under the Charter of Fundamental Rights extend to the obligation, when acting within the scope of EU law, to do so in compliance with obligations under the Charter. The Charter requires, inter alia, that citizens have the right to physical integrity,[8] that they shall not be subject to torture or inhuman or degrading treatment or punishment,[9] that they have the right to privacy,[10] and that they have the right to protection of their personal data from processing without consent or '*legitimate basis laid down by law*.'[11] Governments are required not only to avoid acts which destroy those protections,[12] but also to respect the rights in the course of all actions to which it applies.[13] While the Charter itself only states that compliance is required when States implement EU law, recent jurisprudence of the Court of Justice of the European Union has made clear that the Charter in fact applies more broadly, to action 'in all situations governed by [EU] law,' whether involving the specific implementation of an EU measure or not.[14]

[8] EU Charter, Article 3.
[9] EU Charter, Article 4.
[10] EU Charter, Article 7.
[11] EU Charter, Article 8(1) and 8(2).
[12] EU Charter, Article 54.
[13] EU Charter, Article 51(1).
[14] Case C-617/10 Åkerbeg Fransson (Judgment of 26 February 2013), [19].

CASE STUDY I

Collaboration between UK-German company *Gamma International GmbH* and Swiss company *Dreamlab* in Turkmenistan

Turkmenistan is one of the world's most repressive regimes.[15] Its human rights record has been heavily criticized by various countries and human rights organizations across the world. There is an atmosphere of total repression in the country, which makes it extremely difficult for independent nongovernmental organizations to operate.[16] The climate of fear even extends far beyond Turkmenistan's borders.[17]

Turkmenistani sources have told Amnesty International that people avoid socialising for fear of a misplaced word. All individuals are expected to report any criticism of the state to the authorities and conversations about politics simply do not take place openly.

There is near total control of communications and information. Internet access remains limited and heavily state-controlled. The country's only internet service provider is state-operated, and the Turkmenistani authorities have invested heavily in monitoring internet and telephone communications.[18] Surveillance is significant, and the fraction of the population that does benefit from internet access is closely monitored by state agencies.[19]

The repressive nature of the Turkmenistan Government is well established, and a cursory examination of reports from international human rights organisations should provide any company seeking to conduct business there with multiple issues of concern, or prompt them to review their business partnerships. However, continuing business practices would appear to show that some companies involved in the surveillance industry continue to operate there, with little clarity around how they are approaching human rights risks linked to their business. Leaked contracts show that UK-German company Gamma International GmbH (now trading under the name FinFisher GmbH) together with Swiss company Dreamlab Technologies AG worked in partnership to establish a "an Infection Proxy Infrastructure and Solution applicable nationwide" on the Turkmenistan networks 'Turkmentel' and 'TMCell' in 2011.[20] This partnership included site visits to Turkmenistan, installation procedures and the provision of pricing lists and contact structures as well as payment timelines.

As detailed in a Gamma International brochure describing their suite of systems,[21] FinFly LAN and FinFly ISP are able to infect files that are downloaded by the target, infect the target by sending fake software updates for popular software or infect the target by injecting the Payload into visited websites.[22] The result of such a download is that the computer or mobile phone device is infected, allowing full access to information held on it. It is for instance possible to access emails, social media messaging and Skype calls. It also enables the entity doing the targeting to remotely operate microphones and webcams or cameras on computers and mobile phones.

A Gamma International document specifically relates to the "FinFly ISP Project: Turkmenistan",[23] and the contract material gives a detailed picture of Dreamlab's and Gamma International GmbH's involvement in Turkmenistan.[24] It sets out services including 18 days of network analysis, 40 days of installation of hardware and software, 30 days of on site assembly in Turkmenistan, five-day training for staff, on site system maintenance, coordination meetings, and even software maintenance where necessary.[25] At the time the document was prepared, the deal had, advanced to the stage where specifications were established for the five-day training session including the provision of whiteboards / flipcharts and the requirement that the room be suitably heated or air conditioned by the relevant Turkmeni authorities.[26] The contract material also revealed that visits had been made to Turkmenistan by Nicolas Mayencourt, CEO of Dreamlab, and Thomas Fisher of Gamma.[27]

In April 2014, responding to a draft version of this report, Dreamlab commented that the company "should not [have] been a part of that project, and regret[s] the role [it] played". Dreamlab clarified that it "had nothing to do with the offensive (infection) part of the project", and it "annulled the framework agreement with Gamma International in mid 2011".[28] Although the material does not specifically state that the deal has actually been concluded, researchers of the University of Toronto's " Citizen Lab" have found a FinFisher command & control server in Turkmenistan's Ministry of Communications,[29] indicating that FinFisher has been used and maintained on an ongoing basis.

[15] Human Rights Watch, "World Report 2014, Country Chapter Turkmenistan," available at http://www.hrw.org/world-report/2014/country-chapters/turkmenistan; Amnesty International, "Annual Report 2013 – Turkmenistan," available at http://www.amnesty.org/en/region/turkmenistan/report-2013

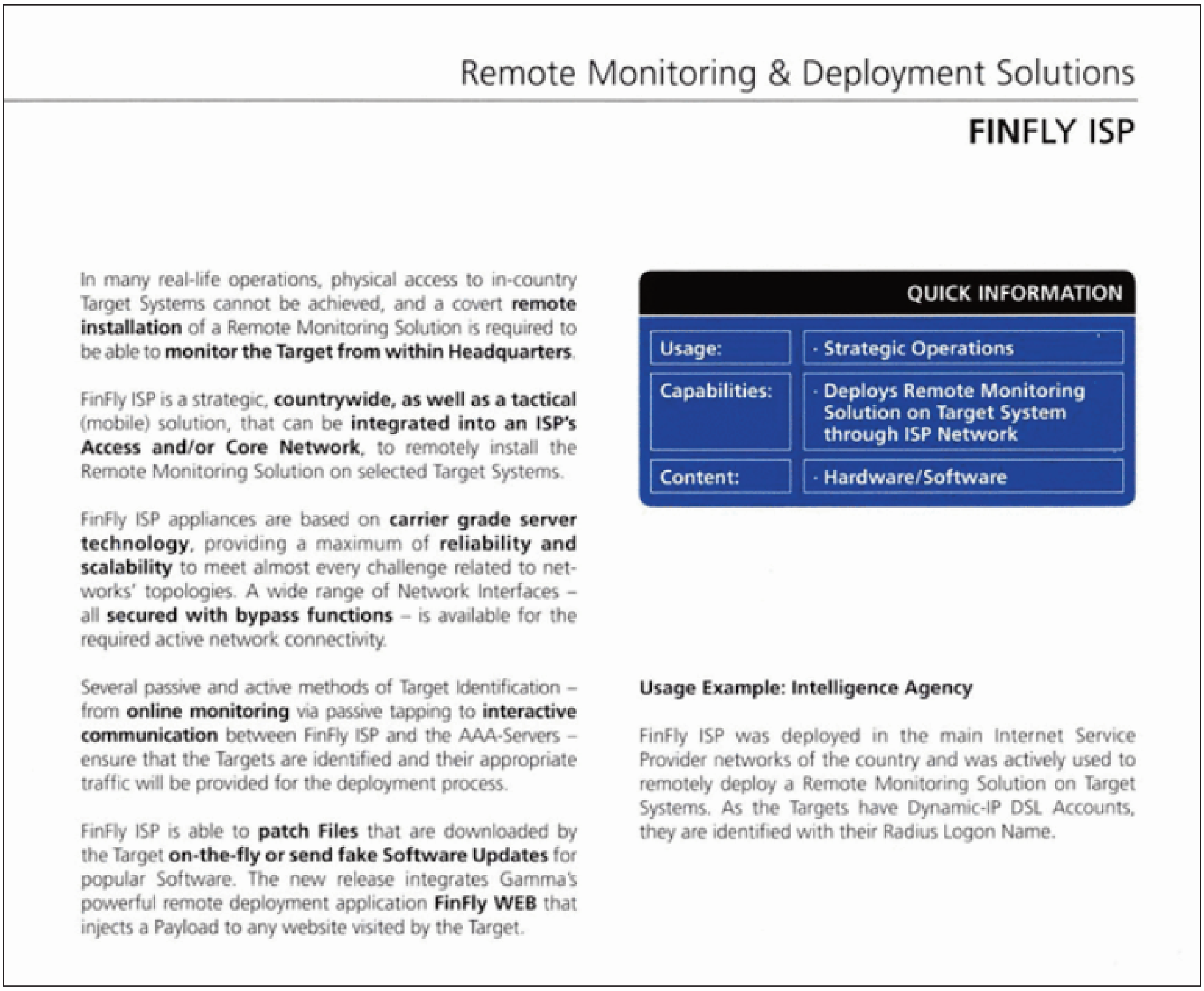
[16] Amnesty International, "Turkmenistan: Total repression ahead of elections," (12 December 2013) available at https://www.amnesty.org/en/news/turkmenistan-total-repression-ahead-elections-2013-12-11

[17] Amnesty International, Turkmenistan: Total repression ahead of elections," (12 December 2013) available at https://www.amnesty.org/en/news/turkmenistan-total-repression-ahead-elections-2013-12-11

[18] Human Rights Watch, "World Report 2014, Country Chapter Turkmenistan," available at http://www.hrw.org/world-report/2013/country-chapters/turkmenistan

[19] OpenNet Initiative, "Turkmenistan," (21 December 2010), available at https://opennet.net/research/profiles/turkmenistan

[20] Dreamlab Technologies "Quotation: Infection Proxy Project 1: Quoted for Gamma International (13 December 2010), available at https://wikileaks.org/spyfiles/docs/DREAMLAB_2010_TMQuotInfe_en.html



Remote Monitoring & Deployment Solutions

FINFLY ISP

In many real-life operations, physical access to in-country Target Systems cannot be achieved, and a covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within Headquarters**.

FinFly ISP is a strategic, **countrywide, as well as a tactical** (mobile) solution, that can be **integrated into an ISP's Access and/or Core Network**, to remotely install the Remote Monitoring Solution on selected Target Systems.

FinFly ISP appliances are based on **carrier grade server technology**, providing a maximum of **reliability and scalability** to meet almost every challenge related to networks' topologies. A wide range of Network Interfaces – all **secured with bypass functions** – is available for the required active network connectivity.

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communication** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic will be provided for the deployment process.

FinFly ISP is able to **patch Files** that are downloaded by the Target **on-the-fly or send fake Software Updates** for popular Software. The new release integrates Gamma's powerful remote deployment application **FinFly WEB** that injects a Payload to any website visited by the Target.

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through ISP Network
Content:	· Hardware/Software

Usage Example: Intelligence Agency

FinFly ISP was deployed in the main Internet Service Provider networks of the country and was actively used to remotely deploy a Remote Monitoring Solution on Target Systems. As the Targets have Dynamic-IP DSL Accounts, they are identified with their Radius Logon Name.

FinFisher brochure describing how it can be integrated into a countrywide network of an Internet Service Provider. Full brochure available at https://www.documentcloud.org/documents/810501-769-gamma-group-product-list-finfisher.html#document/p1/a132141

[21] Gamma Group product brochure: Finfisher: Government IT Intrusion and Remote Monitoring Solutions, available at https://www.documentcloud.org/documents/810501-769-gamma-group-product-list-finfisher.html#document/p1/a132141

[22] Gamma Group product brochure: FinFly LAN: Remote Monitoring and Infection Solutions, available at https://www.documentcloud.org/documents/408439-04-finfly-lan.html

[23] Gamma Group: Finfisher: FinFly ISP Project "Turkmenistan": Installation and Commissioning, available at https://wikileaks.org/spyfiles/docs/GAMMA_2011_TMFinfFinF_en.html

[24] Dreamlab Technologies "Quotation: Infection Proxy Project 1: Quoted for Gamma International, 13 December 2010, available at https://wikileaks.org/spyfiles/docs/DREAMLAB_2010_TMQuotInfe_en.html and Gamma Group product brochure: Finfisher: FinFly ISP Project "Turkmenistan": Installation and Commissioning, available at http://www.wikileaks.org/spyfiles/docs/GAMMA-2011-TMFinfFinF-en.pdf

[24] Dreamlab Technologies "Quotation: Infection Proxy Project 1: Quoted for Gamma International, 13 December 2010, available at http://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-TMQuotInfe-en.pdf

[26] Gamma Group product brochure: Finfisher: FinFly ISP Project "Turkmenistan": Installation and Commissioning, available at http://www.wikileaks.org/spyfiles/docs/GAMMA-2011-TMFinfFinF-en.pdf and http://www.ndr.de/fernsehen/sendungen/zapp/medien_politik_wirtschaft/sicherheitstechnologie103.html

[27] Dreamlab Technologies "Quotation: Infection Proxy Project 1: Quoted for Gamma International, 13 December 2010, available at http://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-TMQuotInfe-en.pdf

[28] Dreamlab's public statement is available at https://www.dreamlab.net/en/statement-concerning-spy-files/

[29] Citizen Lab, "For Their Eyes Only: The Commercialization of Digital Spying" (30 April 2013), available at https://citizenlab.org/2013/04/for-their-eyes-only-2/

CASE STUDY II

Italian company *Hacking Team's* intrusion technology in Morocco and the United Arab Emirates

On Friday July 13, 2012, a group of award-winning Moroccan journalists received a mysterious email, seemingly containing information about a political scandal. It contained a single line in French stating: "Please do not mention my name or anything else, I don't want any problems."[30] Obviously not wanting to miss a potential scoop, the interest of the journalists was triggered. Some of them clicked to open what appeared to be an attached Word document titled *"scandale (2).doc"*.[31]

The journalists in question were part of "Mamfakinch", a citizen media project born in the wake of the Arab Spring protests in Morocco. Aiming at achieving democratic change in Morocco, Mamfakinch was often critical of the Moroccan Government, and was awarded the Google and Global Voices Breaking Borders Award in 2012 for their significant impact in their community on freedom of expression on the internet.[32]

In the same month, sitting in his study in Dubai, human rights activist Ahmed Mansoor received an email titled "very important" in Arabic. Believing he recognized the sender's name, Mansoor opened the attached Word document.[33]

Ahmed Mansoor, a writer, poet, blogger and advocate of political reform, is a prominent critic of the United Arab Emirates (UAE) Government. He highlights incidents of human rights violations and state repression on his blog, which forms a credible source of information for many international and regional human rights organisations.

By opening the email attachments that seemed specifically designed for them, the computers of both the Mamfakinch journalists and Ahmed Mansoor became victims of a malicious software or malware attack.

Once a computer is infected with malware, it is possible for the individual who sent the malware to read all email correspondence, search through documents saved on the computer, and monitor web surfing, including communications via social media. Operators can literally see ideas being formed as they are typed; they have access to family photos, personal correspondence and other sensitive personal information. At this stage, changing passwords or using encryption has no effect on the interception. Some forms of malicious software even allow for the possibility to remotely switch on the microphone and camera of the device (computer / smartphone) so conversations in the vicinity of the computer can be listened to.

Both Mamfakinch and Mansoor, with the help of security experts, were fortunate enough to find out that they had become victims of very intrusive surveillance technology. However, the malware is designed to be totally invisible to the target or anti virus software, leaving countless activists, politicians and journalists across the world vulnerable to the risk of being spied on without them being aware of it.[34] This is not only a grave breach of their privacy, but also undermines their freedom of expression and other human rights.

Researchers of the Citizen Lab, a multidisciplinary research center at the University of Toronto, examined the emails Mamfakinch and Mansoor were sent and were able to retrace them to an Italian company called *Hacking Team* Srl.[35] The malware Mamfakinch and Mansoor were infected with is its flagship product, the Da Vinci Remote Control System. According to *Hacking Team's* senior executive, the company has sold its software to as many as 30[36] to 40[37] countries across five continents. One of *Hacking Team's* representatives added that the software is in use against a few thousand targeted individuals.[38]

[30] "Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d embrouilles"

[31] Slate, "How Government-Grade Spy Tech UsUsed A Fake Scandal To Dupe Journalists" (20 August 2012), available at http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html and Citizen Lab, "Backdoors Are Forever: Hacking Team and the Targeting of Dissent" (October 2012), available at https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

[32] Global Voices, "Announcing the Winners of the Breaking Borders Awards" (2 July 2012), available at http://summit2012.globalvoicesonline.org/2012/07/announcing-the-winners-of-the-breaking-borders-awards/

[33] Bloomberg, "Spyware Leaves Trail to Beaten Activist Through Microsoft Flaw" (10 October 2012), available at http://www.bloomberg.com/news/2012-10-10/spyware-leaves-trail-to-beaten-activist-through-microsoft-flaw.html

[34] Citizen Lab, "Mapping Hacking Team's "Untraceable" Spyware" (17 February 2014), available at https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[35] Privacy International, "Briefing to the Italian Government on Hacking Team's surveillance exports" (15 April 2015), available at https://www.privacyinternational.org/sites/default/files/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team%27s%20surveillance%20exports.pdf.

[36] The Guardian, "Governments turn to hacking techniques for surveillance of citizens" (1 November 2011), available at http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance

[37] L'Espresso, "Noi, I padre del cyber-007" (2 December 2011), available at http://espresso.repubblica.it/dettaglio/noi-i-padri-del-cyber-007%3Cbr-%3E/2167834

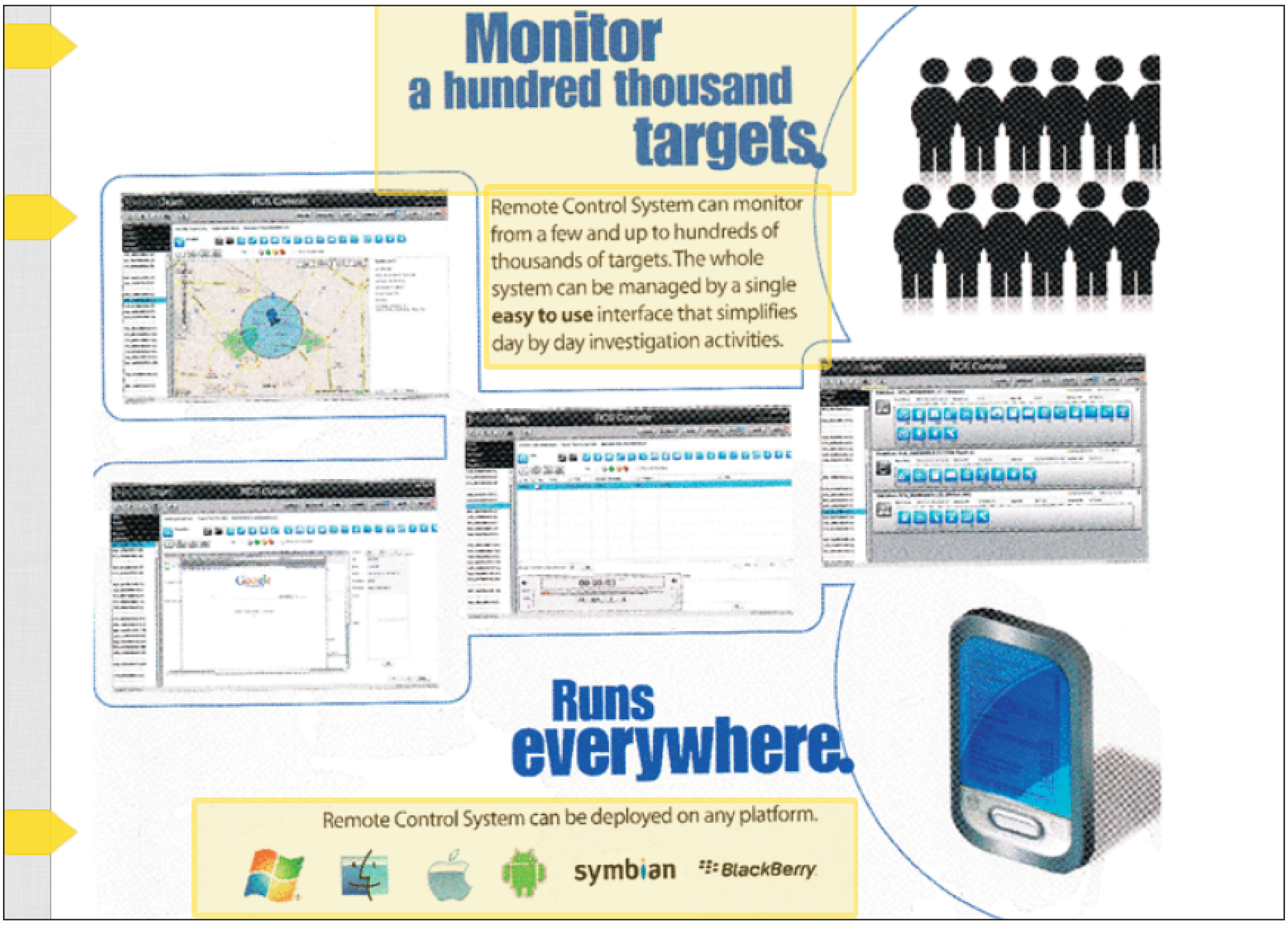
[38] Der Spiegel, "The Transparent State Enemy: Western Surveillance Technology in the Hands of Despots" (8 December 2011), available at http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html

In 2015[39] the marketing materials of *Hacking Team* boast that its malware can “monitor a hundred thousand targets”, allowing the operator to “go stealth and untraceable”, “defeat encryption and acquire relevant data” to “hit your target”.[40]

In April 2014, in response to a draft version of this article, *Hacking Team* advised that:

- it takes specific measures to prevent the misuse of its software, as detailed in its Customer Policy[41]; it “can and [has] suspended software support for [its] software in cases where [it] believed an agency has misused or may misuse the software”; and “[i]t is the nature of law enforcement investigations that they be conducted in confidence, so it is [Hacking Team’s] clients, not *Hacking Team* that must conduct investigations.

As an Italian company, *Hacking Team’s* technologies are now subject to European Union export restrictions. As of 1 January 2015, the EU Dual-Use Regulation 429/2008 restricts the export of intrusion software, defined in a manner that captures the RCS. The EU developments are grounded in agreements made at a 2013 convening of States parties to the Wassenaar Arrangement.[42] As of January 2015, Hacking Team has asserted its immediate compliance with the EU regulation, and has undertaken to seek authorization for exports under the Italian Ministry of Economic Development. However,although the technology is now subject to licensing, it is incumbent on the Italian authorities to appropriately assess whether or not a transfer should be authorised.[43]



Remote Control System can monitor from a few and up to hundreds of thousands of targets. The whole system can be managed by a single **easy to use** interface that simplifies day by day investigation activities.

Remote Control System can be deployed on any platform.

Hacking Team claims that RCS can 'monitor a hundred thousand targets.' Full brochure available at https://www.documentcloud.org/documents/409278-147-hackingteam-rcs.html#document/p2/a68008

[39] Website for ISS World 2014, 2-4 June 2015, Prague: http://www.issworldtraining.com/iss_europe/sponsors.html

[40] Hacking Team, product brochure “Remote Control System. Cyber Intelligence Made Easy”, available at https://www.documentcloud.org/documents/409278-147-hackingteam-rcs.html#document/p2/a68008 See also: https://www.privacyinternational.org/sii/hacking_team/

[41] Website for Hacking Team Customer Policy, available at http://www.hackingteam.it/index.php/customer-policy

[42] Council Regulation (EC) No 428/2009 of 5 May 2009; available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

[43] Hacking Team website, “Hacking Team Complies with Wassenaar Arrangement Export Controls on Surveillance and Law Enforcement/Intelligence Gathering Tools” available at http://www.hackingteam.it/index.php/about-us

CASE STUDY III

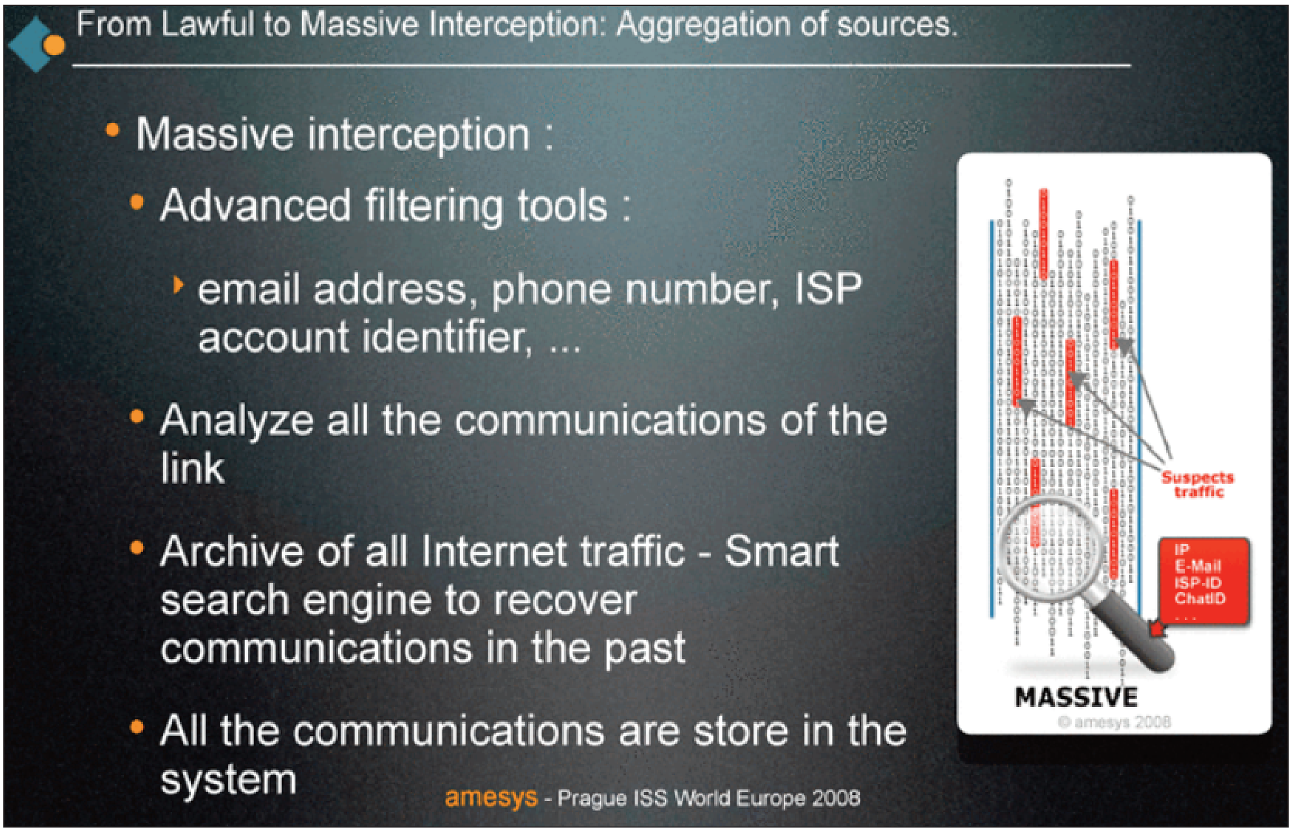
French company *Amesys* and Gaddafi

Amesys, a subsidiary of publicly traded French company Bull SAS, advertises that their internet interception probes can be deployed at many points of communication: Wi-Fi networks, mobile networks, microwave links, satellite links and IP networks. *Amesys* and *Bull* are known to have sold their Eagle monitoring system – a combination of these probes – to the despotic regime of Muammar Gaddafi. The Wall Street Journal reports that the *Amesys* system was "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state".[44]

Amesys is facing an ongoing criminal case into its complicity in acts of torture by the Gaddafi regime.[45] Amesys contends that the Libyan government was an ally of Western government at the time of sale, rendering the sale legitimate. *Amesys* failed to properly investigate likely uses and human rights abuses associated with their product and attempted to disassociate itself from the product by selling it to a company operating in the United Arab Emirates.[46]

As of 1 January 2015, the EU Dual-Use Regulation 429/2008 restricts the export of specialised large-scale IP monitoring systems, such as that sold by *Amesys*. The EU developments are grounded in agreements made at a 2013 convening of States parties to the Wassenaar Arrangement,[47] at which the French government specifically pushed for export controls that would capture *Amesys*' technology. France implemented the control immediately after it was approved by Wassenaar in 2013.

Annex I is a brochure showing the type of surveillance system the new category controls.



From Lawful to Massive Interception: Aggregation of sources.

- Massive interception :
  - Advanced filtering tools :
    - email address, phone number, ISP account identifier, ...
  - Analyze all the communications of the link
  - Archive of all Internet traffic - Smart search engine to recover communications in the past
  - All the communications are store in the system

amesys - Prague ISS World Europe 2008

Slide from Amesys presentation at Intelligent Support Systems for Lawful Interception in 2008, making a distinction between Lawful Intereption and Massive Interception. Full presentation available at https://www.documentcloud.org/documents/409136-21-200810-iss-prg-amesys.html

[44] Wall Street Journal, "Life Under the Gaze of Gadhafi's Spies" (14 December 2011), available at http://online.wsj.com/news/articles/SB10001424052970203764804577056230832805896.

[45] Business & Human Rights Resource Centre, "Amesys lawsuit (re Libya), available at http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496.

[46] Reflets Info, "Advanced Middle East Systems, le Amesys nouveau est de retour en Libye," (24 May 2013), availbale at http://reflets.info/advanced-middle-east-systems-le-amesys-nouveau-est-de-retour-en-libye/.

[47] Council Regulation (EC) No 428/2009 of 5 May 2009; available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

The role of export controls in protecting human rights and promoting transparency

The imposition of export licensing requirements upon strategically chosen, well-defined, surveillance technologies is essential as part of a comprehensive approach to ensuring that such items are not used to for abuses of human rights. Its benefits are primarily two-fold: first, export restrictions can and have stopped specific transfers of equipment where there has been a risk that the transfer would have led to human rights abuses. Second, export controls provide a level of transparency and accountability over a trade in which none currently exist.

While export restrictions are not a silver bullet designed to comprehensively protect human rights, they are a necessary and major component of any successful mitigation strategy. Importantly, even when they are not invoked to restrict a transfer of surveillance technology, export controls also act as an essential accountability and transparency mechanism.

They facilitate the documentation of sales that might otherwise fly under the radar, enabling citizens, the media and civil society to scrutinise and criticise the companies involved in the surveillance trade. The transparency catalysed by the application of export controls to the surveillance industry both increases general knowledge and awareness of the industry, and assists in hold exporting companies and governmental authorities to better account.

CASE STUDY IV

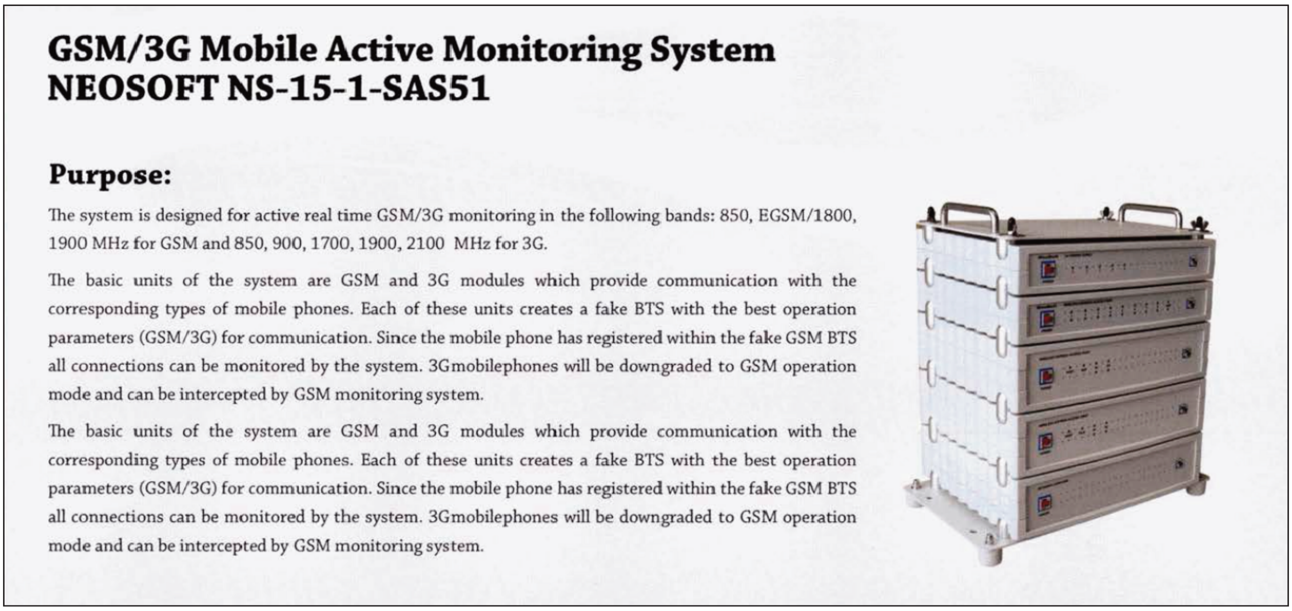
Using export controls to stop transfers of mobile phone monitoring equipment to Bangladesh

Surveillance technology that is used to identify and track mobile phones and intercept calls has been subject to export licensing restrictions for a number of years, through its incorporation into the control list of the Wassenaar Arrangement (see below). Such technology, colloquially known as 'IMSI Catchers' or 'Stingrays', captures mobile phone signals emitted from handsets, by masquerading as a legitimate cell tower or base station, and is manufactured by a wide range of companies across Europe.

In 2009, a UK- based company, Datong, applied to the UK export control authorities for a license to export an IMSI Catcher to an “unnamed south Pacific country,” believed by Privacy International to be Bangladesh. The UK authorities, which currently assess all applications for controlled goods under the EU's Common Criteria, rejected the application on the grounds that it represented a risk to human rights.[48]

The export control authorities in Switzerland have also prevented the export of IMSI Catchers to Bangladesh. In April, 2014 Privacy International published restricted procurement documents showing that a unit of the Bangladeshi police referred to by Human Rights Watch as a “death squad”, the Rapid Action Batallion (RAB), were looking to buy an IMSI Catcher from a company Privacy International believed to be based in Switzerland. RAB have a brutal history and are at the centre of deteriorating human rights situation in Bangladesh; over 700 extrajudicial executions have been carried out by the RAB over seven years since its formation in 2004, according to Amnesty International, while the agency has been explicitly singled out by both the United States and the United Kingdom for continued impunity in regard to human rights violations. The US has recommended that an independent unit be set up to investigate the agency.

After an investigation by Privacy International in conjunction with Swiss magazine WOZ, it was uncovered that representatives from the RAB were being hosted in Zurich by a manufacturer of IMSI Catchers, Neosoft. Swiss authorities have confirmed that they have reason to believe that the RAB representatives were in Zurich to receive technical train-ing from Neosoft on how to use the surveillance technology. NeoSoft's website boasts of its 'academy program', in which 'our instructors will train your staff how to use our software and hardware products'. Because such training would require an export license, and none was sought by NeoSoft, the Swiss export authorities referred the company to federal prosecutors for a potential violation of export control laws. Additional Director General of RAB, Colonel Ziaul Ahsah, subsequently reported to Bangladeshi media that the export had been stopped “just before the shipment of the materials” by Switzerland after allegations that the equipment could be used for human rights abuses.[49]



GSM/3G Mobile Active Monitoring System
NEOSOFT NS-15-1-SAS51

Purpose:

The system is designed for active real time GSM/3G monitoring in the following bands: 850, EGSM/1800, 1900 MHz for GSM and 850, 900, 1700, 1900, 2100 MHz for 3G.

The basic units of the system are GSM and 3G modules which provide communication with the corresponding types of mobile phones. Each of these units creates a fake BTS with the best operation parameters (GSM/3G) for communication. Since the mobile phone has registered within the fake GSM BTS all connections can be monitored by the system. 3Gmobilephones will be downgraded to GSM operation mode and can be intercepted by GSM monitoring system.

The basic units of the system are GSM and 3G modules which provide communication with the corresponding types of mobile phones. Each of these units creates a fake BTS with the best operation parameters (GSM/3G) for communication. Since the mobile phone has registered within the fake GSM BTS all connections can be monitored by the system. 3Gmobilephones will be downgraded to GSM operation mode and can be intercepted by GSM monitoring system.

An IMSI Catcher as retailed by NeoSoft. Full brochure available at http://s3.documentcloud.org/documents/810502/945-neosoft-catalogue.pdf

[48] The Guardian, “Met police using surveillance system to monitor mobile phones,”(30 October 2011), available at http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance.

[49] News Bangladesh, “Switzerland holds back shipping of intelligence gears for RAB,” (12 March 2015), available at http://www.newsbangladesh.com/english/Switzerland%20holds%20back%20shipping%20of%20intelligence%20gears%20for%20RAB/482

The need for an EU-level approach

The EU currently subjects some technology to licensing restrictions because they appear within Annex 1 of the Dual Use Regulation. This list is not decided at the EU level – it incorporates items agreed at international export control regimes. The Wassenaar Arrangement ("WA"), a collection of 41 large exporters of defence and security equipment – including all EU member states – currently contains these surveillance technologies within its list.

Ensuring that all surveillance technologies are incorporated into the WA and then subsequently into the EU Dual Use list is problematic; it takes on some occasions several years, by which time technology often advances or new items appear, and it is based on the ability to accurately define an item. This has proved difficult: in 2013, the WA agreed to add trojans to its list through the articulation of a control on "intrusion software", something which has proved problematic because the agreed language risks inadvertently catching too many items.[50]

While the broad amount of participating states at the WA is welcome (it includes both Russia and the United States), achieving consensus is both time consuming and more difficult than at EU level. Furthermore, as the WA was established at the end of the Cold War and functions similarly to its Cold War predecessor, it focuses on risks to regional and international security and stability related to the spread of conventional weapons and dual-use goods and technologies. Therefore the WA does not consider human rights at all, and it is up to the member states to decide what criteria it should use to assess whether an export should take place. This means that, within the WA, an item cannot not be included in WA control lists solely for reasons related to the protection of human rights.

While the WA is therefore an appropriate and pragmatic forum within which to regulate surveillance technologies, including items unilaterally within the EU dual use control list is both necessary and holds several important advantages.

CASE STUDY V

Export controls increasing transparency and accountability in Switzerland

As a result of a federal review into the issue of exports of surveillance technology in Switzerland, arising out of the Bangladesh case (above), in early 2014 several companies withdrew their applications for licences to export internet monitoring technology from Switzerland. As a result, exports to Ethiopia, Indonesia, Yemen, Qatar, Malaysia, Namibia, two licences for Oman, Russia, Chad, Taiwan, Turkmenistan, UAE, and China did not go ahead.

Due to increased attention surrounding exports of surveillance technologies in Switzerland by media, civil society, and policy makers, in late 2014 the Swiss Government published records of approved and rejected export licenses for all controlled dual use goods, including some surveillance technologies.

According to the records, the Swiss export control authority granted 21 licences for the export of IMSI catchers in 2014; 14 of these were for temporary export and included requirements for re-entry, meaning they were likely used for trade shows or other demonstrations and exhibitions, but seven IMSI catcher licences were for definitive export to Ethiopia, Indonesia, Qatar, Kuwait, Lebanon, Lithuania and Thailand, at a total cost of 8 million CHF (£5.2 million). The impact of this is that individuals, activists, policymakers, researchers, and others are now able to access definitive data on what exports of surveillance technology have been made, both increasing knowledge of the industry and helping hold exporting companies and governmental authorities to better account.

Furthermore, in May 2015, the Swiss Federal Council introduced a major amendment to its export licensing legislation to require Swiss authorities to reject any requests from companies applying to export internet and mobile surveillance technologies from Switzerland if there "are reasonable grounds to believe" that the items could be used for repression in the country of destination.[51]

[50] Comment from Chaos Computer Club e.V. (CCC) for the Joint Public Hearing on Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries in the European Parliament, (21 January 2015) available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/411_horchertexportcontrol_/411_horchert exportcontrol_en.pdf

[51] Swiss government website, available at http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=de&msg-id=57261

The EU – promoter and defender of human rights

The importance of the role of the EU in promoting human rights, at home and abroad, cannot be understated. The soft power of the EU extends into promoting good governance and human rights obligations, which is a key component in an overall export policy, alongside export controls, transparency, and industry due-diligence. In recent years, the major institutions of the EU have issued various statements, initiated action plans, and adopted resolutions on human rights and ICT. For instance, in July 2014, the European Parliament called for a ban on exporting surveillance technology to Egypt, which could be used to spy and repress citizens.[52] This movement has reflected and contributed to the greater international awareness surrounding the problematic increased use of telecommunications and the internet in facilitating human rights abuses.

The EU adopted a Strategic Framework and Action Plan on Human Rights and Democracy in 2012[53] with one of the primary goals being a determination to promote human rights in all areas of its external action "without exception". A goal of similar importance within the Action Plan is to integrate the promotion of human rights into various sectors such as trade, technology and telecommunications, and the Internet. Article 24 on Freedom of Expression Online and Offline requires the inclusion of human rights violations as a reason for broadening export restrictions from member states. Of similar importance, Article 25 refers to the implementation of the UN Guiding Principles on Business and Human Rights.

The European Council took a welcome stronger and clearer position on Article 24 in May 2014, with the adoption of the "EU Human Rights Guidelines on Freedom of Expression Online and Offline.[54]" This included a welcome recognition of the concerning use of surveillance technologies by authoritarian governments and included the EU's promotion of international action to prevent the sale of these technologies to such governments, including by, but notably not solely by, presenting proposals in key multilateral export control regimes. There is no requirement that the EU should be restricted by the limitations set by multilateral export control regimes – either by the technological lists or by the timing of implementation at a national level. The EU should continue to push for greater action at the multilateral level, but there exists significant scope for the EU, whose 28 members make up a significant portion of the membership of 41 countries of the Wassenaar Arrangement, to set a 'higher standard' within the export control regime through the review and amendment of the EU Dual Use Regulation. This higher standard should reflect a more thorough technical analysis and understanding of the technologies and their human rights impact than is currently in operation; a more rigorous examination of the human rights record of the end user; and greater flexibility regarding the addition or removal of specific technologies or definitions on the EU List of Dual Use Technologies.

The EU Human Rights Guidelines also provide an opportunity for the EU to place a strong human rights emphasis in its policy related to technology exports, in stark contrast to the multilateral export control regimes such as the Wassenaar Arrangement. While the Arrangement establishes a mechanism for international consensus on the proliferation of goods from an international security and regional stability perspective, this fails to address the undermining of human rights by the continued proliferation of surveillance technologies. The EU should take the initiative through the opportunities provided by the review of the EU Dual Use export regime, and in light of commitments as part of the Guidelines and previous Council statements to establish clearer and stronger human rights perspectives in its overall policies relating to controlling the export of such technologies.

[52] European Parliament resolution of 17 July 2014 on the situation in Egypt 2014/2728(RSP)

[53] Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy," (25 June 2012), available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

[54] Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (12 May 2014), available at http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf

An agenda for reform

There are five main issues which need to be addressed in order for the EU Dual Use Regulation to effectively safeguard against transfers that pose a risk to human rights:

- **All relevant surveillance technology needs to be subject to licensing;**
- **Human rights implications need to be appropriately considered within assessment criteria;**
- **Disparate national policies facilitating licensing avoidance and potential loopholes in enforcement mechanisms need to be addressed;**
- **Legitimate security research and the development of legitimate security tools need to be exempted from controls and subject to explicit exemptions, and**
- **Controls of encryption and encryption products need to be eradicated.**

1. All relevant surveillance technology is subject to licensing

As stated above, the EU currently subjects some technology to licensing restrictions by virtue of the inclusion of items listed in the Wassenaar Arrangement within Annex 1 of the Dual Use Regulation. However, for the reasons stated above it is essential that the EU develop a mechanism independent of the WA through which to address these issues.

The task of identifying the technologies which might be controlled is being undertaken by a specially formed Subcommittee on ICTs of the Dual Use Working Group – a Commission working group consisting of EU licensing authorities. Simultaneously, the Impact Assessment being conducted by SIPRI and Ecorys aims to provide data on the industry, including values of exports, major destinations etc.

For several years, Privacy International and partners have been collecting restricted brochures, presentations, and marketing material from trade shows and other events in an effort to better understand the industry and surveillance technologies. In order to inform the policy making process, a database containing 1434 different items and links to the scanned brochures is now publicly available here.[55] An example of some of the technologies contained within the database that are not explicitly subjected to export restrictions is available at Annex II.

There are two mutually compatible means by which the Regulation can subject all relevant surveillance technology to licencing.

- **The introduction of EU autonomous lists** would involve member states deciding independently of the WA to control specific surveillance technologies through a list-based system.

- **A dedicated catch-all mechanism** for surveillance technologies would be used for items which do not fall within control lists but which an authority would want to control for a specific reason. If a member state invokes a catch all control, it currently only applies within that member state and to that particular exporter. For example, the catch-all on WMDs at the moment means that if an exporter has been informed by the member state, or if an exporter is aware, that a transfer is for a WMD programme, they need a license.

CAUSE believes that the introduction of an EU autonomous list into the Regulation, combined with a generic catch-all mechanism to "future-proof" the Regulation, are the most appropriate means by which the EU can regulate surveillance technology exports.

Given the civilian nature of some of the technologies, it is difficult and in some cases impossible to accurately define a technology for inclusion into a control list without inadvertently subjecting too many non sensitive or unproblematic items to restrictions. It is therefore essential that further clauses be used to

[55] Privacy International, "Database of Surveillance Technologies", available at https://docs.google.com/spreadsheets/d/15fL62WjeZ2FaMAlsnG37wFrjxk6Q5LLIlWYWmxkQayg/edit#gid=1306600553

define and narrow the items to be controlled. This can be achieved by specifying that an item should only be subjected to licensing restrictions if it is to be deployed for the purposes of electronic surveillance and for the beneficial use of a government entity. While this approach suffers from enforcement difficulties, it is nevertheless still an effective means by virtue of the fact that the vast majority of surveillance technology manufacturers explicitly and exclusively sell their products to government beneficial end-users for the purposes of surveillance, while others exclusively sell solutions to government end users (see Annex III).

2. Human rights implications are appropriately incorporated within assessment criteria, consistent with obligations under the Charter of Fundamental Rights of the European Union.

Although the inclusion of a 'human security approach' to the EU's dual-use export control policy is an improvement on the current system and is well-intended, it may have negative consequences. The Commission Communication states that the approach "may involve evolving towards a notion of 'strategic' items addressing not only and strictly, items with possible military and WMD proliferation end-uses, but taking a wider security approach. This may also imply a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations."

However, "human security" is a concept which so far exists mostly as an academic idea and as such is not well-defined and legally binding. There is no universal agreement as to the meaning and the scope of the concept. There is a risk that adopting this intangible, and not legally binding concept may have unintended consequences, such as narrowing rather than broadening human rights protection. Rather, a "human rights approach" or "human rights-based approach" is preferable.

Human rights are much better defined under international law. There is also a body of well-respected opinion by UN special rapporteurs as well as jurisprudence of international courts which have all adopted a human rights approach to the digital sphere.

Furthermore, the Charter of Fundamental Rights of the European Union, which imposes obligations of compliance on all member states when acting within the scope of EU law and implementing EU law, enshrines, inter alia, the rights to privacy, freedom of expression and the protection of personal data.

If the Dual-Use Regulation mandates an assessment of human rights implications in export assessment criteria, it will be necessary for States to develop implementation guidance in order to ensure human rights implications are addressed in a systematic and standardised manner. Implementation guidance should include, for example, recommendations that States consider:

- the compliance of the destination country with human rights obligations enshrined in the Charter of Fundamental Rights, the European Convention on Human Rights, the International Covenant on Civil and Political Rights and other ratified instruments.
- the human rights record of the beneficial end-user authority, namely the agency or body proposing to purchase the technology;
- the compliance of the export with the eight criteria contained within the 2008 EU Common Position defining common rules governing control of exports of military technology and equipment (EU Common Position); and
- the existence or absence of an appropriate legal framework governing the use of the technology in the destination country, sufficient to ensure that the technology will be used in a manner compliant with human rights.

Implementation guidance should be shared with companies in order to ensure an effective and efficient export process.

3. Disparate national policies facilitating licensing avoidance and potential loopholes in enforcement mechanisms are addressed, and greater transparency of exports is promoted.

This is an important issue as brokers and suppliers based in the EU are able to engage in the trade of surveillance technologies by taking advantage of licensing agencies within the EU with weaker capacity or by manufacturing, operating, and brokering from within the EU but exporting from outside. This is not an issue that is specific to surveillance technologies and is being addressed more broadly within the review process.

Measure to mitigate this include information sharing between EU export and law enforcement authorities, and transparency measures. Specifically for surveillance technologies, there is an urgent need for training, capacity building and increased resources for licensing authorities. Currently, there is limited understanding among licensing authorities regarding the potential utility and effects of different surveillance technologies. This undermines the ability of a licensing authority to make an informed assessment and judgement when deciding whether or not to approve an application.

In order to mitigate against the ability of companies to trade from outside of the EU, it is clear that any effective measures must be as multinational as possible. In this respect, it is important that the European External Action Service and the foreign affairs authorities of member states seek to establish export control measures in multilateral forums, for example within the WA, OSCE, UN, or through independent mechanisms.

Transparency measures must include the full disclosure of data concerning applications for export license for surveillance technologies similar to those already present within the EU Common Position on Arms Exports (1), which stipulates that member states maintain and contribute data to an EU Annual Report concerning exports.[56]

4. Security research and the develop ment of IT security tools are not subject to controls and are subject to explicit exemptions.

One of the major dangers of imposing export controls on surveillance systems is the risk of overreach. While language has to be broad enough to capture the targeted product and its variants, the language must be specific and detailed enough to ensure that no items get inadvertently caught at the same time.

Getting this right is acutely important for security researchers. Export controls can represent a problem for security researchers because it is often difficult to differentiate between IT security research, products used to test deficiencies, and activities and products that are used to actually penetrate systems or devices without consent.

Security researchers need to be able collaborate with one another, across territorial boundaries, and they also need to be able to share their work and problems. The outcome of such research should not be penalized; for example, responsibly disclosing vulnerabilities in hardware and software to vendors and third parties providing information security services, even without public disclosure, or the tools used to discover such vulnerabilities, should never become subject to export controls.

Export controls must be designed and implemented in a manner that preserves the ability of the wider technology community to engage in IT security research and the development of essential communications tools. The unintended impact of chilling free speech and stifling research must be mitigated through narrow and clear language, explicit exceptions for security researchers, and the development of Implementation Guidelines. The Regulation should ensure that controls on surveillance technology are constructed in a narrow and targeted manner and that they only apply to products intended to be deployed for the purposes of electronic surveillance and for the beneficial use of a government entity, so that security research and the development of security tools do not fall under the purview of controls and that research activities are not chilled through ambiguous language.

[56] Council Common Position 2008/944/CFSP, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:EN:PDF

The General Exceptions from licence requirements should make explicit reference to legitimate security research. Implementation Guidance notes should be developed to accompany the Regulation in order to clarify the controls and mitigate the 'chilling effect' that regulation has on individual researchers and smaller companies with limited capacity to interpret export control regulations and implement compliance programmes.

In order to further mitigate the risk of overly broad restrictions, any items made subject to licensing should be narrowly defined as only those specially designed and marketed for use in intelligence gathering and law enforcement by and for the benefit of governmental agencies.

Government should consult with industry and civil society to promote implementation of “know your customer” policies that will reduce the potential for approved, or otherwise permissible, exports to misappropriated for the abuse of human rights.

5. Controls of encryption and encryption products should be eradicated.

Some surveillance equipment and software currently falls within the scope of controls because of the strength of cryptography used. This particularly relates to products that fall within categories 5A002 and 5D002 of the Wassenaar Arrangement. EU member states and authorities such as the External Action Service should seek to eradicate all export controls on cryptography, particularly within the Wassenaar Arrangement. Reporting requirements should also be eradicated.

Cryptography is a key security measure to protect the confidentiality of communications, and to also ensure trust and confidence in digital interactions. In addition to undermining the security of networks and devices, their continued control is a major burden to licensing agencies given that they make up by far the largest proportion of controlled equipment. They further disadvantage European companies, for example telecommunications companies competing with countries with no licensing restrictions, with little gain for protecting national security given the wide availability of cryptography to armed non-state groups and other actors.

Annex I: IP network communications surveillance systems or equipment

The agreed language means that surveillance systems which fulfill all of the following criteria are now subject to licensing restrictions:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):

  a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));

  b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and

  c. Indexing of extracted data; and

2. Being specially designed to carry out all of the following:

  a. Execution of searches on the basis of 'hard selectors'; and

  b. Mapping of the relational network of an individual or of a group of people.it can also be used to monitor circuit switched (telephone) networks

ETI Group was a Danish company producing Evident, a comprehensive surveillance system. In 2010 ETI was bought by the large British defence contractor BAE for $212

The Evident system would require a license when used for carrier class IP networks, and fulfilling all of the other criteria.

The full brochure is available at https://www.documentcloud.org/documents/711361-brochure539.html

Annex II: Examples of surveillance technologies not currently subject to explicit export licensing restrictions[57]

1. Lawful Interception Solutions & Inter-connectors

Utimaco (Germany) Lawful Interception Management System (LIMS) https://www.documentcloud.org/documents/804664-1233_utimaco_product-description.html

2. Monitoring Centres & Voice Identification[58]

VasTech (South Africa) Zebra https://s3.amazonaws.com/s3.documentcloud.org/documents/711299/brochure484.pdf

Speech Technology Center (Russia) VoiceGrid X https://s3.amazonaws.com/s3.documentcloud.org/documents/810314/803-glimmerglass-product-description-intelligent.pdf

3. Probes and Fibre Taps

Utimaco (Germany) Access Points https://www.documentcloud.org/documents/804661-1247-utimaco-product-description-lims-access.html

Telesoft Technologies (UK) Hinton Interceptor http://www.documentcloud.org/documents/267027-telesoft-technologies-hinton-5000-interceptor.html

Glimmerglass (USA) Intelligent Optical Solutions https://s3.amazonaws.com/s3.documentcloud.org/documents/810314/803-glimmerglass-product-description-intelligent.pdf

4. Location Monitoring

Verint (Israel, UK, Germany, Cyprus, Netherlands) SkyLock https://www.documentcloud.org/documents/885760-1278-verint-product-list-engage-gi2-engage-pi2.html#document/p12/a135329

Telesoft Technologies (UK) Hinton Abis Probe https://s3.amazonaws.com/s3.documentcloud.org/documents/711319/brochure504.pdf

[57] Some of these items may be subject to licensing under other categories of items, for example if they employ specific types and levels of encryption.

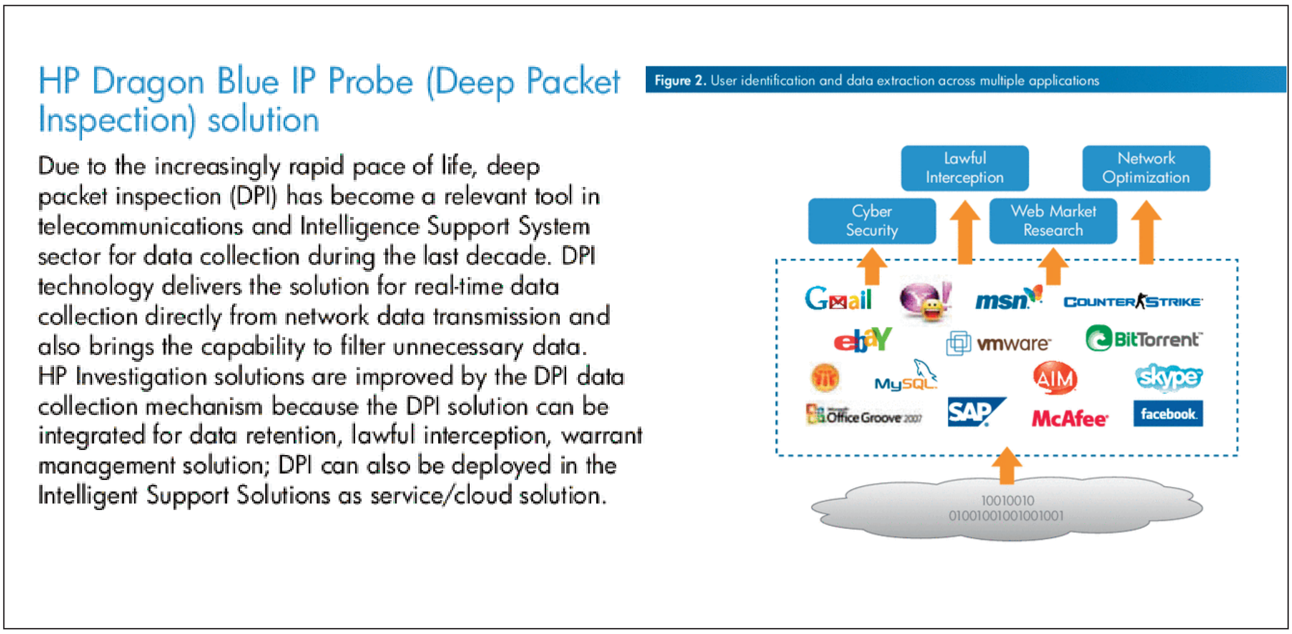
[58] Some monitoring centres were added to the WA dual-use list in 2013 as category 5.A.1.j. However, the category only applies to a narrow set of monitoring centre solutions which fulfill all of the criteria within the category, and only to IP monitoring centres. ETI's Evident shown in Annex I, for example, can also monitor circuit switched networks.

Annex III: Hewlett Packard Deep Packet Inspection (DPI) Technology

Modern telecommunications networks necessarily rely on technology within the infrastructure that manages the flow of packets throughout the network and monitors their contents. This is necessary not only to manage the network, but also to ensure that the packet contains no malicious contents that undermine the security of a network. Some items can employ a method known as Deep Packet Inspection (DPI) to monitor packets. While such a method can be entire legitimate and necessary, it can also be employed by products for the surveillance of communications for security and law enforcement purposes. Narus, an American company, for example, sold DPI technology to Egypt before the Arab Uprising which allowed the security services to monitor internet activity in real time during the Uprising.[59] Narus' marketing vice president claims that "Anything that comes through (an Internet protocol network), we can record...We can reconstruct all of their e-mails along with attachments, see what web pages they clicked on; we can reconstruct their (Voice Over Internet Protocol) calls."[60]

Subjecting such items to export control restrictions by simply defining what the technology would however be impossible given its legitimate uses. For example, the multinational IT company Hewlett Packard manufactures several type of probes employing DPI techniques for various purposes. From their brochure below, it is clear that the technology can be employed for various purposes, including Lawful Interception.

In such circumstances, it is only through clauses specifying for which particular end-uses and beneficial end-users an exporter would require a license that such items can be subjected to licensing restrictions. In order for such an approach to be effective, end-use assurances would need to be undertaken by the exporter from customers and distributors.



HP Dragon Blue IP Probe (Deep Packet Inspection) solution

Due to the increasingly rapid pace of life, deep packet inspection (DPI) has become a relevant tool in telecommunications and Intelligence Support System sector for data collection during the last decade. DPI technology delivers the solution for real-time data collection directly from network data transmission and also brings the capability to filter unnecessary data. HP Investigation solutions are improved by the DPI data collection mechanism because the DPI solution can be integrated for data retention, lawful interception, warrant management solution; DPI can also be deployed in the Intelligent Support Solutions as service/cloud solution.

Figure 2. User identification and data extraction across multiple applications

https://www.documentcloud.org/documents/810666-849-hewlett-packard-product-description-blue.html

CAUSE