

# Sorveglianza, Spaghetti e Mandolino

Claudio Guarnieri  
@botherder

wiretapmeifyoucan@jabber.ccc.de

OTR: ACAD067C 5C6DBD0C 45D7BDC6 25B1404A 5E216E91



INTERNET  
MONITORING



PHONE  
MONITORING



TROJAN



SPEECH  
ANALYSIS



SMS  
MONITORING



GPS  
TRACKING

FRANCE

GERMANY

ITALY

UK

# SPY FILES



OWNI

The Washington Post

L'Espresso

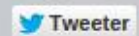
THE BUREAU  
OF INVESTIGATIVE  
JOURNALISM

ARD®

THE  
HINDU



Powered by  
OWNI



30





TO: State Security Investigation Department  
Cairo  
Egypt

OFFER NO: 0610 FF-GUK-061  
DATE: Tuesday June 29, 2010  
CUSTOMER ID: EGY-SSD  
PAGE: 6 / 12

CONTACT PERSON	REFERENCE	SHIPPING METHOD	SHIPPING TERMS	DELIVERY	PAYMENT TERMS	VALIDITY
Johnny Debs	JD	Air Freight	CIP	6-8 weeks	As per Terms & Conditions	1 month

ITEM #	DESCRIPTION	MODEL	QTY
A	Remote Intrusion Solution		
1	FinSpy		
1.1	FinSpy Software		
1.1.1	FinSpy Proxy License	FSPL	1
	FinSpy Master License	FSML	
	FinSpy Generation License	FSGL	
1.1.2	FinSpy Agent License (per client)	FSAGL	2
1.1.3	FinSpy Activation License:	FSPCAL	10

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)
A	Remote Intrusion Solution			
1	FinSpy			
1.1	FinSpy Software			
1.1.1	FinSpy Proxy License	FSPL	1	188,549.00
	FinSpy Master License	FSML		
	FinSpy Generation License	FSGL		
1.1.2	FinSpy Agent License (per client)	FSAGL	2	12,887.00
1.1.3	FinSpy Activation License: - Windows - OSX (Q4/2010)	FSPCAL	10	2,646.00
	Including FinSpy lifeline Support: FinSpy Update & Upgrade (Year 1)			
1.2	FinSpy Hardware			
1.2.1	FinSpy Master Server	FSM	1	6,112.00
1.2.2	FinSpy Agent Workstation	FSAG	2	1,112.00
1.2.3	FinSpy Common & Spare Parts	FSC	1	12,223.00
1.4	FinSpy - Installation & Training			
	FinSpy Installation and Product Training Number of Students: 2-4	FSTI	1	19,445.00

# British firm offered spying software to Egyptian regime – documents

Gamma International's Finfisher program would have enabled government spies to monitor activists and censor websites

[Share](#)  
[Tweet this](#)  
[Email](#)

**Karen McVeigh**

The Guardian, Thursday 28 April 2011 14.05 BST



[Print this](#)  
[Share](#)  
[Contact us](#)

Send to a friend

Sender's name

Recipient's email address

Your IP address will be logged

Share

Short link for this page:

<http://gu.com/p/2zmx3>

[StumbleUpon](#)

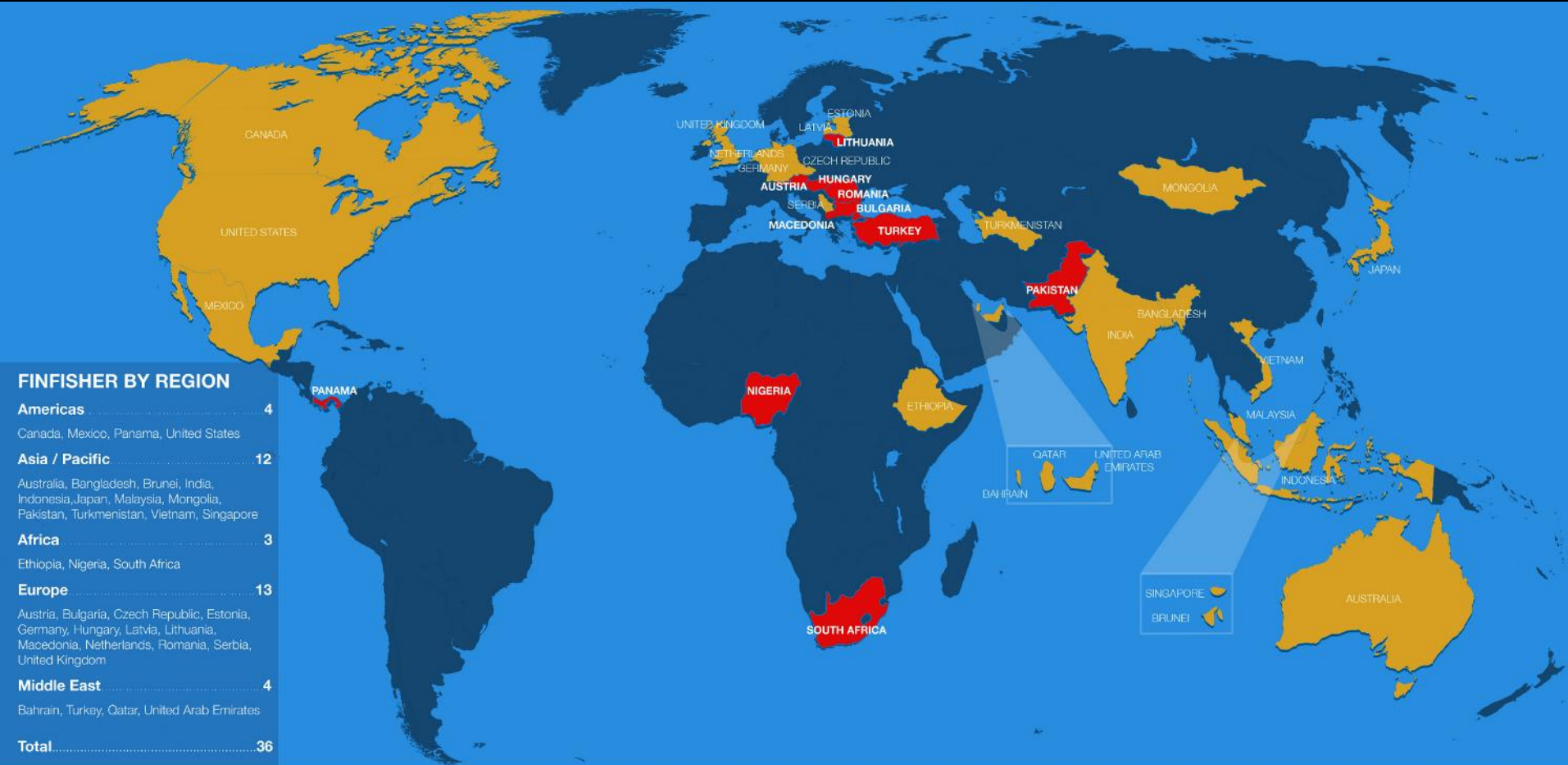
[reddit](#)

[Tumblr](#)

WikiLeaks

SPY FILES





**SCAN RESULTS**



The map shows the results of scanning for characteristics of FinFisher Command & Control servers, and analysis of Internet Census Project data.

- (1) This may not be a full representation of all active FinFisher servers due to scanning methodology and possible concealment strategies.
- (2) Presence of a server does not necessarily indicate knowledge or complicity by the country as proxies are undoubtedly in use on some FinFisher deployments.

**FINFISHER'S GLOBAL PROLIFERATION: APRIL 2013 UPDATE**

© AUTHORS: MORGAN MARQUIS-BOIRE, BILL MARCZAK, CLAUDIO GUARNIERI & JOHN SCOTT-RAILTON  
 MAP: JOHN SCOTT-RAILTON  
 CITIZEN LAB

Australia, Austria, **Bahrain**, Bangladesh,  
**Brunei**, Bulgaria,  
Canada, Czech Republic, Estonia, **Ethiopia**,  
Germany, Hungary, India, Indonesia, Japan,  
Latvia, Lithuania, Macedonia, Malaysia,  
**Mexico**, Mongolia, Netherlands, **Nigeria**,  
**Pakistan**,  
Panama, Qatar, Romania, Serbia, Singapore,  
South Africa, **Turkey**, **Turkmenistan**, United  
Arab Emirates, United Kingdom, United  
States, Vietnam



# Turkmenistan declares an era of happiness

Turkmenistan has announced “an era of supreme happiness” to mark the start of Kurbanguly Berdymukhamedov’s second term as president.



Kurbanguly Berdymukhamedov at his inauguration last month as Turkmenistan's president Photo: AFP/GETTY

# MCMC investigates The Malaysian Insider for spyware reports

Bernama

Friday, March 15, 2013



MCMC said The Malaysian Insider have failed to verify the report from The New York Times and had made its own conclusion on the matter (Graphic by Dayang Norazhar/ The Mole)

CYBERJAYA: Malaysian Communications and Multimedia Commission (MCMC) is investigating the news report issued by local online news portal, The Malaysian Insider, at around 3:00 pm yesterday with the headline stating "Malaysia Uses Spyware against Own Citizens, NYT Reports".

MCMC would like to state that this report is speculative and ill- researched.

*SULIT - untuk kegunaan dalaman sahaja*

**SENARAI CADANGAN CALON PRU KE-13 MENGIKUT NEGERI**  
 (sila rahsiakan)  
 (PARLIMEN & DUN)

**KELANTAN**


BAHAGIAN	BILANGAN	SENARAI CALON YANG DIHANTAR		
PARLIMEN	14	PASIR MAS, KOTA BHARU, KETEREH, KUBANG KERIAN, KUALA KRAI, BACHOK, PENKALAN CHEPA, PASIR PUTEH, RANTAU PANJANG, TANAH MERAH, MACHANG, TUMPAT, GUA MUSANG (13)		
KAWASAN	NAMA CALON	KEKUATAN	KELEMAHAN	STATUS SEMASA
PARLIMEN PASIR MAS	DATO' HAJI HANAPI BIN MAMAT (KETUA BAHAGIAN PASIR MAS)			DIMINATI OLEH MASYARAKAT DI PASIR MAS DAN MEMPUNYAI SUMBER KEWANGAN YANG KUKUH
PARLIMEN KOTA BHARU	MOHAMAD FATMI CHE SALLEH (KETUA BAHAGIAN KOTA BHARU)	MENDAPAT SOKONGAN AKAR UMBI MESRA MASYARAKAT		
<i>PARLIMEN KETEREH</i>	YB DATUK MD ALWI HJ CHE AHMAD (ADUN KOK LANAS, TIMBALAN KETUA BAHAGIAN KETEREH)			
PARLIMEN KUBANG KERIAN	AZLAN BIN ABDULLAH (AJK BAHAGIAN KUBANG KERIAN)	MESRA MASYARAKAT GOLONGAN MUDA SOKONGAN DARI BAHAGIAN		


# Indonesian Top Internet Service Providers Accused of Spying on Users



Mar 18, 2013 at 19:30 PM by Enricko Lukman, in Web

Discussion: 0

 Author's RSS

 This RSS

Three Indonesian Internet Service Providers (ISPs) [Telkom](#), [Biznet](#), and Matrixnet Global are somewhat under fire now as they will face [15-year imprisonment charges](#) if they are proven guilty of spying on their users. This incident came under scrutiny after the University of Toronto Munk School of Global Affairs Citizen Lab published [a report last week](#) which found that as many as 25 countries are infected by the remote intrusion and surveillance software [FinSpy](#).

With FinSpy, people can capture information from an infected computer, like passwords and even Skype calls. The program should have



Credit: [slidingmind.com](#)

# Corruption scandal reveals use of FinFisher by Mexican authorities

BY: ALINDA VERMEER ON: 22-JUL-2013

SHARE:   



Following reports that the Mexican prosecution authority appears to be not only using FinFisher, but also to be involved in a corruption scandal surrounding the purchase of this intrusive surveillance technology, the Mexican Permanent Commission (composed of members of the Mexican Senate and Congress) has urged Mexico's Federal Institute for Access to Public Information and Data Protection (IFAI) to **investigate** the use of spyware in Mexico.

The corruption scandal, which entails the price of the surveillance technology being **purchased at more than double** the market rate, revealed that the Mexican government had bought FinFisher from Obses, a company which has been on the receiving end of dozens of no-bid governmental projects.

While we don't know if Obses purchased the malware from Gamma International, the British company that developed FinFisher, this is the first instance we are aware of where a reseller was involved in the sale of FinFisher. The standards of international responsible business conduct of the OECD guidelines however remain relevant even if a reseller is selling its products.

EQUIPO BALÍSTICO

EQUIPO ANTIMOTÍN

EQUIPO TÁCTICO

DRONES

## EQUIPO TÁCTICO





**NEWS**

**IMAGES**

**VOICES**

**SPORT**

**TECH**

**LIFE**

**PROPERTY**

**ARTS + ENTS**

**TRAVEL**

**MONEY**

[UK](#) ▾ / [World](#) ▾ / [Business](#) ▾ / [People](#) ▾ / [Science](#) / [Environment](#) ▾ / [Media](#) ▾ / [Technology](#) / [Education](#) ▾ / [Images](#) /

[/ Appeals](#)  
[News](#) > [UK](#) > [Crime](#)

## Ethiopian political refugee living in London alleges he was victim of 'unprecedented example of espionage on British soil'



# Ethiopian refugee 'illegally' spied on using British software

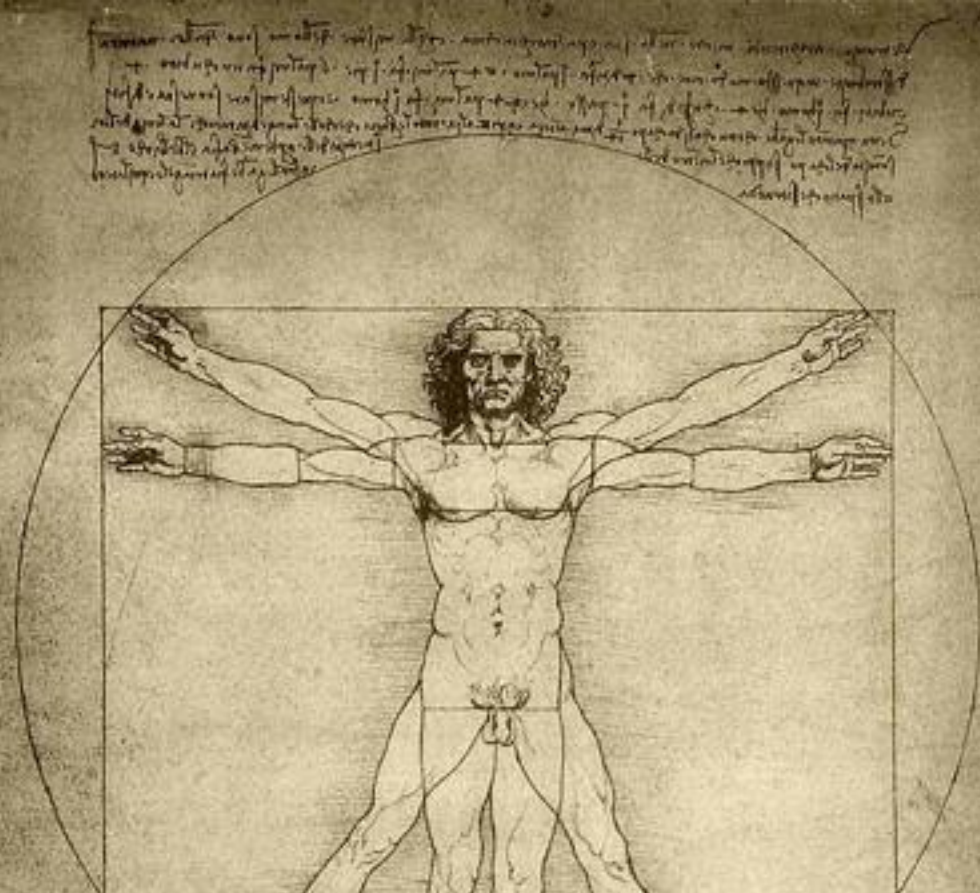
POLITICS / 17 FEBRUARY 14 / by LIAT CLARK ↗

A privacy group has announced that an Ethiopian political refugee living in the UK was illegally targeted from overseas using British-made spy software. It has brought the claim to the attention of the National Crime Agency for investigation.

This is not the first time London-based group Privacy International has honed in on the potential for harm caused by FinFisher spy software, made by UK firm Gamma International. In the past it has appealed to HMRC and foreign governments to carry out investigations into the potential misuse of a UK export it says is used to suppress












Go  
STEALTHY Acquire  
**DEFEAT** ANT  
encryption.  
A SECRET  
agent.




**Thousands** of encrypted  
communications per day.  
Get them, **in clear**.



**MEXICAN CIRCUIT**

**MOROCCAN CIRCUIT**

-  **Hong Kong** HK Broadband Network Ltd.  
14.136.236.xxx
-  **London** Linode  
176.58.102.xxx
-  **Amsterdam** GleSYS  
31.192.228.xxx
-  **Atlanta** Linode  
50.116.32.xxx
-  **Mexico** UniNet  
200.67.230.xxx

-  **Kiev** Electro-City LLC  
91.222.36.xxx
-  **Tampa** NOC4 Hosting  
74.50.126.xxx, 74.50.126.xxx
-  **Morocco** Maroc Telecom (ONPT)  
62.251.128.xxx

# HACKING TEAM RCS

Suspected Government Users Worldwide

## Citizen Lab 2014

Bill Marczak, Claudio Guarneri, Morgan Marquis-Boire & John Scott-Railton




## 21 SUSPECTED GOVERNMENT USERS

AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico Colombia Panama	Hungary Italy Poland	Oman Saudi Arabia UAE	Egypt Ethiopia Morocco Nigeria Sudan	Azerbaijan Kazakhstan Malaysia Thailand South Korea Uzbekistan

### CAUSE FOR CONCERN

 **52%** (in bold) fall in the bottom 3rd of a World Bank ranking\* of freedom of expression and accountability

 **29%** are in the bottom 3rd for Rule of Law

\*World Bank 2012 WGI

Mexico, Colombia, Panama,  
Hungary, Italy, Poland, Turkey,  
**Oman, Saudi Arabia, UAE, Egypt,**  
**Ethiopia, Morocco, Nigeria,**  
**Sudan, Azerbaijan, Kazakhstan,**  
Malaysia, Thailand, South Korea,  
**Uzbekistan.**

## How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists

By Ryan Gallagher | Posted Monday, Aug. 20, 2012, at 9:00 AM

Share 57

Like 72

Tweet 211



EMAIL



PRINT



COMMENT

4



Pro-democracy demonstrators in Morocco

Photo by FADEL SENNA/AFP/GettyImages

An email claiming to reveal a political scandal will grab the attention of almost any journalist. But what if the email was just a ruse to make you download government-grade spyware designed to take total control of your computer? It could happen—as a team of award-winning Moroccan reporters recently found out.

[Mamfakinch.com](#) is a citizen media project that grew out of the Arab Spring in early 2011. The popular website is critical of Morocco's [frequently draconian](#) government, and [last month](#) won an award from Google and the website [Global Voices](#) for its efforts "to defend



## **Hisham Almiraat**

Co-founder of **Mamfakinch**.

Director of **Global Voices**

**Advocacy**.

# Ahmed Mansoor

Prominent blogger from **UAE**.  
Member of UAE Five.







Rabe saw the problem from another perspective. "Let me just suggest that somebody who figures out how the Hacking Team software works and publishes that on the internet is doing a great favor to terrorist organizations, criminals, and others, because investigation underway will be compromised," he said. This was a clear allusion to the work of independent security researchers like his co-panelist Guarnieri and the absent Marquis-Boire.

<http://www.theverge.com/2013/3/12/4090444/the-spy-within-researchers-hackers-spar-over-state-sponsored-malware>

## Statement on Citizen's Lab/Kaspersky report of June 24, 2014:

Hacking Team is aware of the ongoing efforts of Citizen's Lab [sic] to attack our business by attempting to disclose confidential information, systems, and procedures that we use. This report is only their latest effort. It is evident that the primary complaint of the authors is about repressive government, however, Citizen's Lab has chosen to target a private business operating in full compliance with all relevant law.

We believe the software we provide is essential for law enforcement and for the safety of us all in an age when terrorists, drug dealers, sex traffickers and other criminals routinely use the Internet and mobile communications to carry out their crimes. We sell only to government agencies such as police forces. We do not conduct digital investigations. Those are carried out by law enforcement and are, of course, entirely confidential as is any law enforcement investigation.

The June 24 report does not include our customer policy, however, we invite you to read the policy which describes the steps we take to avoid abuse of our software. We believe this policy is unique in our industry and a strong, good-faith effort to prevent misuse of our products. We have both refused to do business with agencies we felt might misuse our software, and we have investigated cases either discovered internally or reported in the press that suggest abuse. We can and have taken action in such cases, however, we consider the results of our investigations and the actions we take based on them to be confidential matters between us and our clients.

Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. . . . Although it is clear that many States possess offensive intrusion software, such as Trojan technology, the legal basis for its use has not been publicly debated in any State, with the exception of Germany.

# Elusive FinSpy Spyware Countries

By NICOLE PERLROTH

## This Powerful Spy Software Is Being Abused By Governments Around The World

MICHAEL KELLEY | MAY 2, 2013, 4:01 PM

Recommend 933 | Share 206

## Software Meant to Fight Crime Is Used to Spy on Dissidents

the guardian | TheObserver



News | US | World | Sports | Comment | Culture | Bus

## Offshore company directors military and intelligence re

News > World news > Surveillance

Companies making use of offshore secrecy i supplied surveillance software used by repre

## UK firm faces questions over how spyware ended up in Bahrain

Human right International

Bloomberg

Our Company | Professional | Anywhere

Jamie Doward The Observer,

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTA

## Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy

activists.

Full list

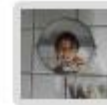
GMT



# Mexico: Advocates Demand Investigation of FinFisher Spyware

Posted **21 June 2013** 6:58 GMT

Categories: **Advocacy, Campaign, Human Rights, Law, Mexico, Privacy, Surveillance**



Written by  
**Renata Avila**

 This post also available in  
**Español · México: Activistas**

## Privacy rights violations challenged in Lahore High Court

posted by  **Admin** on  **Wed, 05/08/2013 - 14:44**



IFAI, Mexico. Photo by

**Islamabad, May 8, 2013:** Bytes for All (B4A), Pakistan had been following up on "FinFisher" for almost last one year with grave concern for its implications on citizens' privacy and larger human rights in the country. B4A had some evidence of its presence in the country but not enough to share publicly. It was not until the investigations and findings by its two partners [Citizen Lab](#) and [Privacy International](#) revealed FinFisher's active deployment on [PTCL](#) Network that triggered mass reaction.

Striving to safeguard the digital and privacy rights of the citizens of Pakistan, Bytes for All has taken prompt action against the recently discovered spyware, moving the Lahore High Court through an appropriately focused Writ Petition. The petition focuses on the increasing threats to citizen privacy, absence of individual protections, and the violations of basic human rights granted by the country's constitution. It questions the authorities about the motives of existence of this anti-democracy and predatory technology in the country.

FinFisher is notorious for targeting human rights movements all over the world and has advanced spying and surveillance capabilities for invading into the privacy of anyone connected to the Internet or mobile. The technology is obnoxious, and can even surreptitiously turn on people's webcams, listen to Skype, and control computers remotely.

B4A along with the larger civil society movement in the country is now reaching out to the court of justice, requesting to take notice of such outrageous violations of fundamental human rights that are in complete contradiction of constitution of Pakistan and any acceptable norms of civil liberties. We expect that the honorable court will look into this issue with utmost care, and bring the violators to justice.

Pakistani citizens have the right to know that why authorities in Pakistan are invading their privacy and at what costs on

## Läti peaminister: jälgimisprogramm FinSpy võib olla siin kasutusel (15)

13. juuni 2013 11:55



Toimetas: Matti Aivar Lind

www.DELFI.ee

Läti peaminister [Valdis Dombrovskis](#) ütles märtsis, et iga riik mõtleb küberkaitsele ja et paljud peavad seda väga oluliseks. Riigimehe sõnul ei saa seetõttu välistada, et jälgimisprogrammi ka Lätis kasutatakse, vahendas uudisteagentuur LETA.



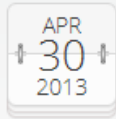
Reuters/Scanpix

Läti televisiooni (LNT) telesaates "900 sekundit" rääkinud Dombrovskise ütles, et ta ei saa riigi salajast jälitustarkvara lähemalt kommenteerida, kuid ei välista, et jälitusprogrammi [FinSpy](#) riigis kasutatakse.

"Ma ei välista, et taolised meetodid võivad olla kasutusel, kuid need [jälgimisprogrammid] on Lätis kindlalt kontrollitud ja jälgitud," ütles peaminister.

# The Mozilla Blog

News, notes and ramblings from the Mozilla project



## Protecting our brand from a global spyware provider



Alex Fowler

21

A [recent report](#) by [Citizen Lab](#) uncovered that commercial spyware produced by Gamma International is designed to trick people into thinking it's Mozilla Firefox. We've sent Gamma a cease and desist letter today demanding that these illegal practices stop immediately.

As an open source project trusted by hundreds of millions of people around the world, defending Mozilla's trademarks from this type of abuse is vital to our brand, our users and the continued success of our mission. Mozilla has a longstanding history of protecting users online and was [named](#) the Most Trusted Internet Company for Privacy in 2012 by the Ponemon Institute. We cannot abide a software company using our name to disguise online surveillance tools that can be – and in several cases actually have been – used by Gamma's customers to violate citizens' human rights and online privacy.

It's important to note that the spyware does not affect Firefox itself, either during the installation process or when it is operating covertly on a person's computer or mobile device. Gamma's software is entirely separate, and only uses our brand and trademarks to lie and mislead as one of its methods for avoiding detection and deletion.

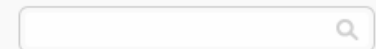
Through the work of the Citizen Lab research team, we believe Gamma's spyware tries to give users the false impression that, as a program installed on their computer or mobile device, it's related to Mozilla and Firefox, and is thus trustworthy both technically and in its content. This is accomplished in two ways:



### About Alex Fowler

Alex leads privacy and public policy for Mozilla

[More from Alex »](#)



### About This Blog

The Mozilla Blog is the official source for Mozilla-related news, opinions, events and more.



Stop  
Digital Arms  
Trade



Tell your  
representative



Sign  
the petition



Share

**Imagine  
you are planning a peaceful protest to confront the current  
regime in your country.**





# HOW EUROPE EQUIPS THE WORLD WITH SURVEILLANCE TECHNOLOGY

## WHAT WE WANT TO CHANGE ABOUT IT

## AND WHY WE NEED YOUR SUPPORT

140 signs on Twitter can be enough to trigger mass demonstrations against repressive authoritarian regimes.

A single Facebook post has the power to bring human rights violations to the surface that would otherwise have remained hidden.

**One sentence on an online blog, however, can also mean PRISON, TORTURE and DEATH.**

Indeed, spyware technology MADE IN EUROPE has allowed governments around the world to closely monitor activists and human rights defenders.

[SIGN OUR PETITION!](#)



# Digital spy tech could face same regulation as weapons in international treaty

By [Josh Lowensohn](#) on December 4, 2013 08:07 pm [Email](#) [@Josh](#)

DON'T MISS STORIES *FOLLOW THE VERGE*



Like

334k

Follow

395K followers



HEADLINES



Full restaurant  
now show up  
search results



Google fights  
Muslims' take  
in copyright b



Connecticut w  
its successful  
website plan t  
other states



The Enemies of Internet  
Special Edition : Surveillance

Introduction

State Enemies

Corporate Enemies

Amesys

Blue Coat

Gamma International

Hacking Team

Trovicor

# Corporate Enemies

## 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 DaVinci, is able, it says, to break encryption on emails, files and Internet telephony protocols....

]HackingTeam[

# OECD complaint against Gamma International accepted for further investigation

BY: [ALINDA VERMEER](#) ON: 24-JUN-2013

SHARE: [t](#) [f](#) [g+](#)



In an encouraging first response to our complaint against surveillance company Gamma International (Gamma), the UK National Contact Point (NCP) of the Organisation for Economic Cooperation and Development (OECD) announced that it will **further investigate our claim against Gamma**, as the evidence submitted appears to substantiate our allegations.

In February 2013, Privacy International, together with the European Center for Constitutional and Human Rights, Bahrain Watch, the Bahrain Center for Human Rights and Reporters without Borders **filed a complaint** against Gamma for breaching no less than eleven of the OECD guidelines by exporting its surveillance technology to Bahrain, where this technology was allegedly used to target human rights activists. The OECD guidelines promote responsible business conduct, and cover a range of issues including the impact a company's business in a certain country has on human rights. They apply to all multinationals including those whose products, business partners or countries carry a higher risk of abuse.

The NCP stated that the evidence that we submitted supports our allegations about human rights risks in Bahrain, that these risks are likely to have been known to Gamma, and that Gamma's product may have been used to target Bahraini activists. According to the NCP, this substantiates the issues in respect of the company's obligations to do

# Privacy International seeking investigation into computer spying on refugee in UK

17-FEB-2014

SHARE:   



Privacy International today has made a criminal complaint <sup>[1]</sup> to the National Cyber Crime Unit of the National Crime Agency urging them to investigate the potentially unlawful interception of the communications of an Ethiopian political refugee living in the UK, as well as the role a British company played in developing and exporting invasive **commercial surveillance software** called FinSpy.

Tired of living under constant surveillance and harassment, Tadesse Kersmo and his wife left Ethiopia and arrived in the United Kingdom in 2009 where they were subsequently granted asylum.

In April 2013, Mr. Kersmo became aware of a report published by the Citizen Lab, an interdisciplinary research lab at the Munk School of Global Affairs of the University of Toronto, that mentioned a spyware campaign targeting Ginbot 7 members. The report, titled **"You Only Click Twice: FinFisher's Global Proliferation"**, describes how pictures of Ginbot 7 members included in an email were used as bait to infect computers with the Trojan FinSpy. One of the pictures included in the email was of Mr. Kersmo who is a member of the Ginbot 7 executive committee.

A subsequent analysis by Privacy International and Bill Marczak, a research fellow at the Citizen Lab, of Mr Kersmo's computer suggests that in June 2012, three years after escaping persecution, his computer appears to have been infected with the commercial surveillance spyware FinSpy.



## Press Releases

[February 2014](#)[January 2014](#)[December 2013](#)[November 2013](#)[October 2013](#)[September 2013](#)[August 2013](#)[July 2013](#)[June 2013](#)[May 2013](#)

February 18, 2014



## American Sues Ethiopian Government for Spyware Infection

### Months of Electronic Espionage Put American Citizen and Family at Risk

Washington, D.C. - An American citizen living in Maryland sued the Ethiopian government today for infecting his computer with secret spyware, wiretapping his private Skype calls, and monitoring his entire family's every use of the computer for a period of months. The Electronic Frontier Foundation (EFF) is representing the plaintiff in this case, who has asked the court to allow him to use the pseudonym Mr. Kidane – which he uses within the Ethiopian community – in order to protect the safety and wellbeing of his family both in the United States and in Ethiopia.

# Privacy International files criminal complaint on behalf of Bahraini activists targeted by spyware FinFisher

Published on 13 October 2014 in Press releases

Countries: Bahrain, United Kingdom

Campaigns: Big Brother Inc.



Privacy International today has made a criminal complaint to the National Cyber Crime Unit of the National Crime Agency, urging the immediate investigation of the unlawful surveillance of three Bahraini activists living in the UK by Bahraini authorities using the **intrusive malware** FinFisher supplied by British company **Gamma**.

Moosa Abd-Ali Ali, Jaafar Al Hasabi and Saeed Al-Shehabi, three pro-democracy Bahraini activists who were granted asylum in the UK, suffered variously from years of harassment and imprisonment, and were subject to unspeakable torture at the hands of the Bahraini government.

**Investigation and analysis by human rights group Bahrain Watch** showed that while Moosa, Jaafar, and Saeed were residing in the UK, Bahraini authorities targeted the

activists and had their computers infected with the surveillance Trojan FinFisher.



INTERNET MONITORING

PHONE MONITORING

TROJAN

SPEECH ANALYSIS

SMS MONITORING

GPS TRACKING

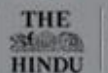
- BRAZIL
- CANADA
- CHINA
- COLOMBIA
- CZECH REPUBLIC
- DENMARK
- FRANCE
- GERMANY
- HUNGARY
- INDIA
- ISRAEL
- ITALY**
- NETHERLANDS
- NEW ZEALAND
- POLAND
- SOUTH AFRICA
- SWITZERLAND
- TURKEY
- UK
- UKRAINE
- US

**Italy** ✕

**7 companies**

Innova	🔍 Files	📞 📱	✉️ 📍
BEA	🔍 Files	📞 📱	
Ips	🔍 Files	📞 📱	
RCS		📞 📱	
Resi group		📞 📱	
Hacking Team	🔍 Files		☠️
Loquendo	🔍 Files		👤

# SPY FILES





## Internet interception and probes



The development of IP network and the increasing use of internet-based services led Law Enforcement Agencies to new investigation needs and to the use of advanced products for IP communication interception.

In order to satisfy these needs, Innova Research & Development Laboratories have developed a complete range of effective and reliable products and solutions for the interception of any kind of protocols and IP-based communication, such as web browsing, e-mail and web-mails, social networks, peer to peer communication, chat and videochat etc..

Moreover, a team of specialized researchers is committed to decode new communication protocols, developing updated products for any IP communication interception and identifying effective solutions for any LEA investigation need.



## LAWFUL INTERCEPTION

PRODUCTS

Advanced products and capabilities:

- Monitoring Centre
- Voice Interception
- IP Decoding
- Relation Analysis
- Text Analysis
- Voice Biometrics
- Geo Fencing
- ...

[Read more](#)



## UNCONVENTIONAL IP INTELLIGENCE

PRODUCTS

Products and capabilities for:

- Monitoring Centre
- Network Monitoring
- DPI
- Meta Data Extraction and Analysis
- Data Retention
- Cyber Security
- OSINT
- IT Intrusion
- Social Network Intrusion
- Man in the Middle Attacks
- HTTPS decoding

- Profiling

[Read more](#)



## Voice Biometrics – Public Security Solutions

Nuance offers intelligence agencies, military and law enforcement organizations with powerful speech solutions that accurately identify individuals of interest using text-independent voice biometrics, as well as identify conversations of interest via technologies such as language, gender and keyword detection. Nuance Public Security Solutions deliver real-time alerting while monitoring telecommunication networks, select public places or in-field activities through mobile devices. Post-processing capabilities for investigation and forensic purposes are also available.

[Learn more about Nuance Public Security Solutions](#)



## PRODOTTI

Una grande esperienza in primo piano.

Sono tre le categorie di Clienti che si affidano all'esperienza RCS:

- **Autorità Giudiziaria e Forze dell'Ordine** - Utilizzano essenzialmente dispositivi e apparecchiature per il monitoraggio telefonico e ambientale su vasta scala. Operano principalmente nelle Sale Ascolto delle 167 Procure della Repubblica.
- **Corpi Speciali** - Sviluppano attività mirate e specializzate, operando in un ambito tecnologico sofisticato, in campi d'azione specifici.
- **Servizi Segreti e Intelligence** - Le loro necessità si concentrano su piccole apparecchiature dedicate all'intercettazione diretta di singoli bersagli, al trattamento e alla decodifica dei dati ottenuti.



# Finmeccanica sold radio equipment to Syria: report

ROME | Thu Jul 5, 2012 4:37pm EDT

0 COMMENTS



Tweet

7



Share



Share this



g+1



0



Email



Print

## RELATED NEWS

[Defection cheers anti-Assad coalition at Paris meet](#)

[Finmeccanica sold radio equipment to Syria: report](#)

[WikiLeaks says starts releasing hacked Syria emails](#)

[Syria pummels rebels as battered city collects bodies](#)

[Syrian army attacks rebels, Turkey scrambles F16s](#)

## ANALYSIS & OPINION

[End the assault on female and local journalists](#)

[Julian Assange's fall from the heavens](#)

## RELATED TOPICS

(Reuters) - A unit of Italian defense technology group Finmeccanica sold sophisticated communications equipment to Syrian police as recently as February, an Italian weekly reported on Thursday, quoting emails published by Wikileaks.

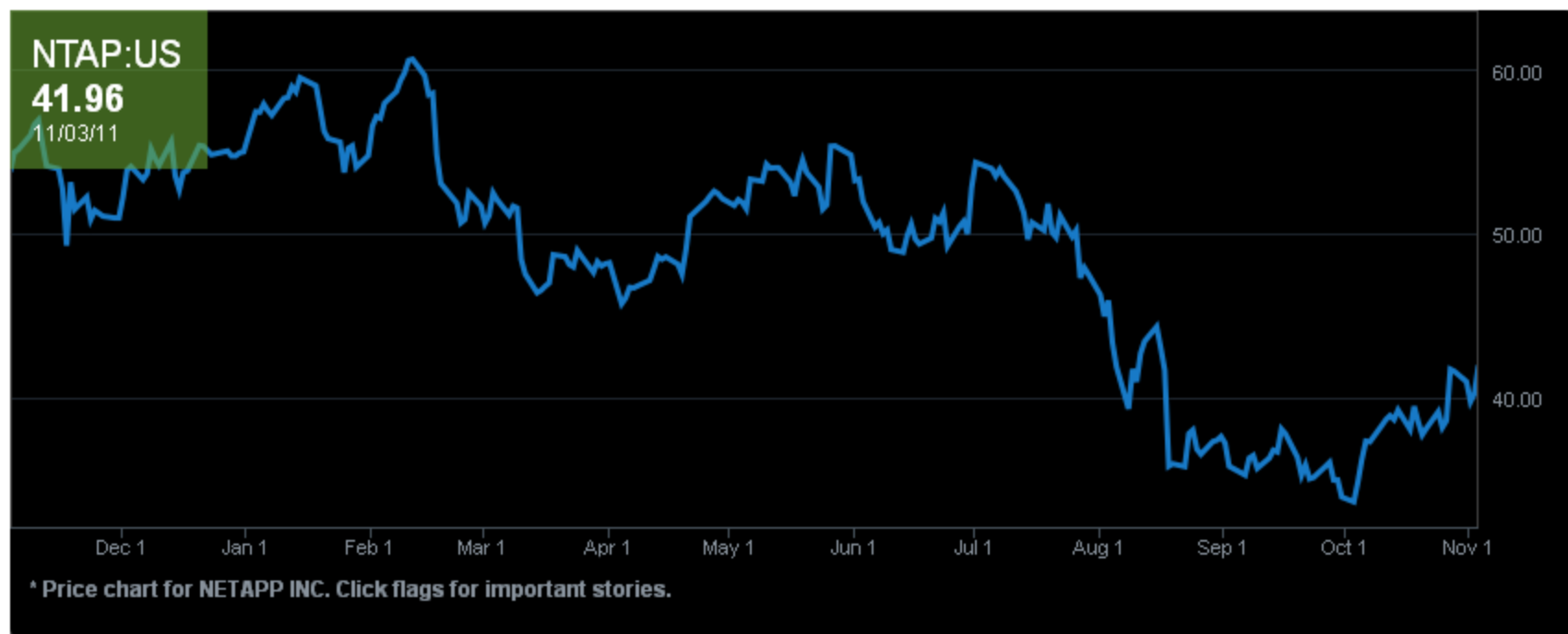
According to l'Espresso, Finmeccanica's Selex Elsag unit sold Syrian authorities its Tetra mobile communications equipment, a system used by military, police and emergency services as well as companies and other organizations.

Tetra allows secure, encrypted communications from vehicles and helicopters. L'Espresso said the technology was classified as "dual use" for civil and military, but the company said in a statement it was designed and sold for civil use only.

The technology "was designed for use by emergency responders," the company said. The Tetra technology "was conceived for this function," it said.

# Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear

By Ben Elgin and Vernon Silver | Nov 4, 2011 12:01 AM GMT+0100 | [0 Comments](#) [Email](#) [Print](#)



[Home Page](#) >> [Europe](#) >> [France](#)

## FRANCE

[English](#) | [français](#)[Surveillance](#)[Syria](#)

11 April 2014

### France: Opening of a judicial investigation targeting Qosmos for complicity in acts of torture in Syria

More than 18 months after FIDH and LDH filed a complaint before the Prosecutor of the Paris Court denouncing the alleged implication of French companies, in particular Qosmos, in the selling of surveillance material to Bachar El Assad's regime, FIDH and LDH welcome today's decision to open a judicial investigation for complicity of acts of torture in Syria.

This investigation has been attributed to the specialised unit in crimes against humanity and war crimes created in January 2012 within the Paris Tribunal.

This new development follows the opening, in May 2012, of another judicial investigation into the alleged implication of the French company Amesys for complicity to acts of torture in Libya. It is the second time that French judicial authorities agree to investigate the alleged involvement of an ICT company which sold surveillance material to an authoritarian regime.

Qosmos, a company specialised in supplying Deep Packet Inspection, material designed for real



International News 24/7



WATCH LIVE

Open

COMING UP

- 11:27: WEATHER
- 11:30: NEWS
- 11:45: THE BUSINESS INTERVIEW

WATCH AGAIN

11:16 (Paris time) IN THE PAPERS

TOP STORIES

SHOWS

FRANCE

AFRICA

MIDDLE EAST

EUROPE

AMERICAS

ASIA / PACIFIC

SPORTS

BUSINESS / TECH

CULTURE

DOCUMENTARIES

IN DEPTH



France

torture | Muammar Gaddafi | Libya

# French firm Amesys probed over 'complicity in torture'

 Share 5
  Tweet 34
  Share 0
  Share 5

0







# Bureau of Industry and Security

U.S. Department of Commerce

Where Industry and Security Intersect

Search...

- Home
- About BIS
- Regulations
- Licensing
- Enforcement
- Compliance & Training
- Policy Guidance
- Add'l Programs
- Reform

## Newsroom

- Newsroom
- Press Releases
- Speeches
- Testimony
- Publications
- Electronic FOIA
- Export Control Reform News
- Archives

## Reform

- Reform
- Export.Gov
- ECR Teleconference
- Decision Tree Tools
- ECR FAQs

### Italian Company Agrees to \$100,000 Penalty for Unlawful Technology Export to Syria

| Print |

FOR IMMEDIATE RELEASE

BUREAU OF INDUSTRY AND SECURITY

Wednesday, September 17, 2014

Office of Congressional and Public Affairs

[www.bis.doc.gov](http://www.bis.doc.gov)

202-482-2721

### Italian Company Agrees to \$100,000 Penalty for Unlawful Technology Export to Syria

WASHINGTON – The U.S. Department of Commerce's Bureau of Industry and Security (BIS) today announced that Area S.p.A. (Area), located in Italy, has agreed to a \$100,000 civil penalty settling charges that it knowingly sold U.S.-origin network monitoring equipment to the Syrian Telecommunications Establishment (STE) without the required U.S. Government authorization.

In February 2011, Area sold a Central Monitoring System (CMS) to STE. The CMS is capable of collecting data about web surfing, emails, online chatting, and Voice-over-Internet Protocol (VOIP). In the hands of the Syrian Government, the system could be used to further the repression of the Syrian people.

The sale of the CMS to STE, which contained minimal U.S. content, was not subject to the Export Administration Regulations. However, Area subsequently transferred U.S.-origin network monitoring equipment to STE to monitor and test the CMS. This subsequent transfer required U.S. Government authorization, which was not obtained. Area purchased the network monitoring equipment, valued at approximately \$140,000, from a company located in San Mateo, California. Area personnel hand-carried the equipment from Italy to Syria and then installed and provided training for STE. Area knew at the time of the transfer that U.S. export regulations prohibited the unlicensed transfer of U.S.-origin items to Syria.

Area cooperated with BIS in its investigation.

BIS controls exports and reexports of commodities, technology, and software to support national security and foreign policy ,

# Did Hacking Team receive Italian public funding?

BY: [KENNETH PAGE](#) ON: 03-MAR-2014

SHARE: [t](#) [f](#) [g+](#)



Only a few days after it was reported that intrusive surveillance technology developed and sold by Italian surveillance company Hacking Team was found in some of the most repressive countries in the world, Privacy International has uncovered evidence which suggests the company has received over €1 million in public financing.

It has come to Privacy International's attention that Hacking Team appears to have received €1.5 million from two venture capital funds originating from the Region of Lombardy in 2007. One of the funds, [Finlombarda Gestioni SGR S.p.A](#) (FGSGR) has only a single shareholder - Finlombarda S.p.A, a public financial services agency whose [only shareholder is the Region of Lombardy](#). Finlombarda S.p.A. designs, builds and manages financial services on behalf of the Region of Lombardy, placing the profits of Hacking Team hand-in-hand with the public finances of Lombardy. FGSGR also lists the Head of Venture Capital as being a Board Member of Hacking Team itself.

Given the countries where Hacking Team's products appeared to have been identified, and that the company is potentially being financed with public money, Privacy International today written to over 175 members of the Italian Parliament and senior Italian Government authorities [urging them to investigate and to take action](#) to ensure that its invasive and offensive not exported from Italy and used in human rights violations.

**Hacking Team technology identified in repressive regimes**

