

# Marriage from Hell

*On the Secret Love Affair Between Dictators and  
Western Technology Companies*

By Evgeny Morozov @ 28C3

# Disclaimer

*This is not a comprehensive overview –  
more than a hundred companies  
involved*

# Bloomberg: Wired for Repression

## The Technology

### United States

NetApp Inc. and Hewlett-Packard Co. gear to Syria. Blue Coat Systems Inc., McAfee Inc. and NetApp products to Tunisia.

### Finland

Nokia Siemens Networks to Iran and Tunisia.

### Sweden

Ericsson AB mobile-positioning gear to Iran.

### Denmark

ETI A/S data interception gear to Tunisia.

### Ireland

AdaptiveMobile Security Ltd. message retrieval/storage to Iran.

### United Kingdom

Creativity Software Ltd. location tracking gear to Iran.

### France

Qosmos SA scanning probes to Syria. Amesys technology to Libya.

### Germany

The former Siemens AG business now known as Trovicor GmbH to nations including Egypt, Syria, Tunisia, Yemen, Bahrain, Morocco and Pakistan. Utimaco Safeware AG to Tunisia, Syria.

### Italy

Area SpA headed installation in Syria that was cancelled in November.

## The Victims



## The Buyers

### Syria

A system being installed under the direction of Syrian intelligence agents would have intercepted, scanned and cataloged virtually every e-mail through Syria.

### Iran

Even as Iran pursued a brutal political crackdown, including arrests and executions surrounding its contested 2009 elections, companies supplied it with location tracking and text-message monitoring equipment that turn mobile phones into tools for surveillance.

### Bahrain

Computers loaded with Western-made surveillance software generated transcripts wielded in the interrogations of scores of detainees.

### Tunisia

Aided directly and indirectly by American and European suppliers, the Tunisian government took control of virtually all the country's electronic communications, even changing the content of e-mails in transit.

*Sources: Series reporting included review of 150 documents, and interviews with dozens of current and former company employees, government officials, and dissidents who were targeted. Assistance from reporter Alan Katz in Paris.*

Read the Bloomberg series [Wired For Repression](#).

# SpyFiles

The image shows the SpyFiles website interface. At the top, there are five monitoring options: INTERNET MONITORING (highlighted with a red border), PHONE MONITORING, TROJAN, SPEECH ANALYSIS, SMS MONITORING, and GPS TRACKING. Below these is a world map with a red outline. On the left side of the map, there is a vertical list of countries: BRAZIL, CANADA, CHINA, COLOMBIA, CZECH REPUBLIC, DENMARK, FRANCE, GERMANY, HUNGARY, INDIA, ISRAEL, ITALY, NETHERLANDS, NEW ZEALAND, POLAND, SOUTH AFRICA, SWITZERLAND, TURKEY, UK, UKRAINE, and US. At the bottom of the page, there is a footer with logos for WikiLeaks, OWNI, The Washington Post, l'Espresso, THE BUREAU OF INVESTIGATIVE JOURNALISM, ARD, THE HINDU, and a Privacy icon. To the right of the footer, there is a 'Powered by OWNI' logo and social media sharing options for Twitter (195 tweets) and Facebook (3k likes).

# Wall Street Journal – Censorship Inc

## CENSORSHIP INC.

17 1 11  
Like +1 Tweet



### Life Under the Gaze of Gadhafi's Spies

A Libyan reporter's tangle with the Libyan surveillance apparatus shows how U.S. and European interception technology could instead be deployed against dissidents, human-rights campaigners, journalists or enemies of the state.

### Video >

#### Finding New Ways to Keep Tabs on People

The global market for off-the-shelf surveillance technology has taken off in the decade since 9/11. WSJ's Jennifer Valentino-DeVries explains some of the new methods governments and law enforcement are using to monitor people. [Video](#)

### Reactions to Censorship Inc.

#### U.S. Restricts Firm for Web Filter Sale to Syria

The U.S. Department of Commerce is placing restrictions on a person and a company in the United Arab Emirates for supplying Syria with Internet-filtering devices made by California-based Blue Coat Systems.

#### Nokia Siemens to Trim Iran Ties

Nokia Siemens Networks said it won't take on new business in Iran and will gradually reduce its existing commitments.

#### Bill Aims to Curb Tech Firms' Exports

Pressure mounted Thursday on U.S. and Western companies that sell censorship and surveillance technology to repressive regimes, with Rep. Chris Smith introducing a bill that would restrict such exports.

- [Digits: Clinton Criticizes Sale of Surveillance Tools](#)
- [Pressure Mounts to Limit Surveillance Exports](#)

#### Bill Would Curb Exports of Spy Software

Legislation to be introduced in the House would bar sales of equipment that could be used for online censorship or surveillance to any country that restricts the Internet.



#### Huawei to Scale Back in Iran

Chinese telecom-equipment maker Huawei Technologies will scale back its business in Iran, following reports that Iranian police were using mobile-network technology to track down and arrest



Inside Libyan Unit



Surveillance Catalog



Censorship in Syria

# Complex & diverse use

1. Monitoring & manipulation of email and SMS (keyword-based, user-based, location-based)
2. Filtering of online content
3. “Intelligent” video surveillance (+voice analysis)
4. Spying on a user's computer activity (potentially even planting evidence)
5. Surveillance as harassment (Tunisia: porn images in work-related emails)

**I. Can't We Just Ban Them?**

# “Bans” work only if they are global

1. Blue Coat (US) → distributor (UAE/”Iraq”?) → Syria
2. Allot (Israel) → distributor (Denmark) → Iran
3. NetApp (US) → Area Spa (Italy) → Syria

# ...but we can still raise the costs

Want to save this for later? [Add it to your Queue!](#)

## U.S. Bans UAE Company for Supplying Internet Filter to Syria

By William McQuillen - Dec 15, 2011 11:39 PM GMT+0300

[ADD TO QUEUE](#)

[Recommend](#) 1  
[Tweet](#) 23  
[Share](#) 2  
[+](#) 0  
More  
[Print](#) [Email](#)

The U.S. Commerce Department banned a United Arab Emirates company from receiving items under the jurisdiction of U.S. export controls after it was found to have shipped Internet filtering devices to Syria.

The devices, made by [Blue Coat Systems Inc. \(BCSI\)](#) of Sunnyvale, California, can be used to block pro-democracy websites and identify activists as part of Syrian President Bashar al-Assad's crackdown against dissidents, the department said today in a statement.

Waseem Jawad, using the company names Infotec and Info Tech, ordered multiple Blue Coat devices in December 2010 from an authorized distributor in the UAE. The devices ended up in Syria, according to the Commerce Department.

Related News: [Europe](#)

Want to save this for later? [Add it to your Queue!](#)

## European Union Bans Exports to Syria of Systems for Monitoring Web, Phones

By Vernon Silver - Dec 1, 2011 9:57 PM GMT+0300

[ADD TO QUEUE](#)

[Recommend](#) 7  
[Tweet](#) 370  
[Share](#) 28  
[+](#) 3  
More  
[Print](#) [Email](#)

The European Union barred exports of surveillance technology to [Syria](#) following reports the regime was procuring and using such gear.

"Exports of equipment and software intended for use in the monitoring of internet and telephone communications by the Syrian regime," are banned, the 27-nation bloc said today in a statement that included other restrictive measures.

[Enlarge Image](#)



Bloomberg News reported Nov. 4 that an Italian company, Area SpA, was building a surveillance system that would have given

# But what about beyond US/EU?

*Washington Post's* report from a surveillance fair in the US counted reps from 43 countries

→ How do we know what happens to US or German surveillance gear that is destined for, say, Moldova or South Sudan (whose rep was spotted at the Malaysian fair...)?

# What Would Viktor Do?



# Another note on sanctions...

Broad sanctions = Bad, As They Harm Users (and Govts Mostly Get Away)

Narrow sanctions = Good, But Often Ineffective

Example: Syria

# Know-Your-Customer rules

1. What can we learn from other controversial industries?  
[e.g. it's probably harder to open an account with a US bank than to buy surveillance gear from a US firm]
2. Forcing companies selling censorship & surveillance gear to do (continuous) due diligence on clients
3. Foreseeing modifications and customizations
4. After-sale configurations & support: NetApp/Area case

# How much of this could/should be delegated to technology?

1. Viability of remote kill switches & refusal to run updates based on location
2. Required periodic monitoring of where services are used (Websense & its 40,000 customers)
3. How easy would it be to defend this rhetorically, as we are fighting surveillance with more surveillance?

## **II. What to Anticipate**

# Too soon to call victory even in parts of the Middle East

- Libya: new government started social filtering of the Web
- Tunisia: DPI is still in use, waiting for govt's regulation (but censorship is more transparent)
- Egypt: the military go after individual bloggers

# Ex-USSR: Pushback after the Arab Spring

online independent newspaper  
the**moscow**news

## **CSTO wants to monitor the internet to prevent a repeat of Arab revolutions**

by *Evgeniya Chaykovskaya* at 13/09/2011 18:06

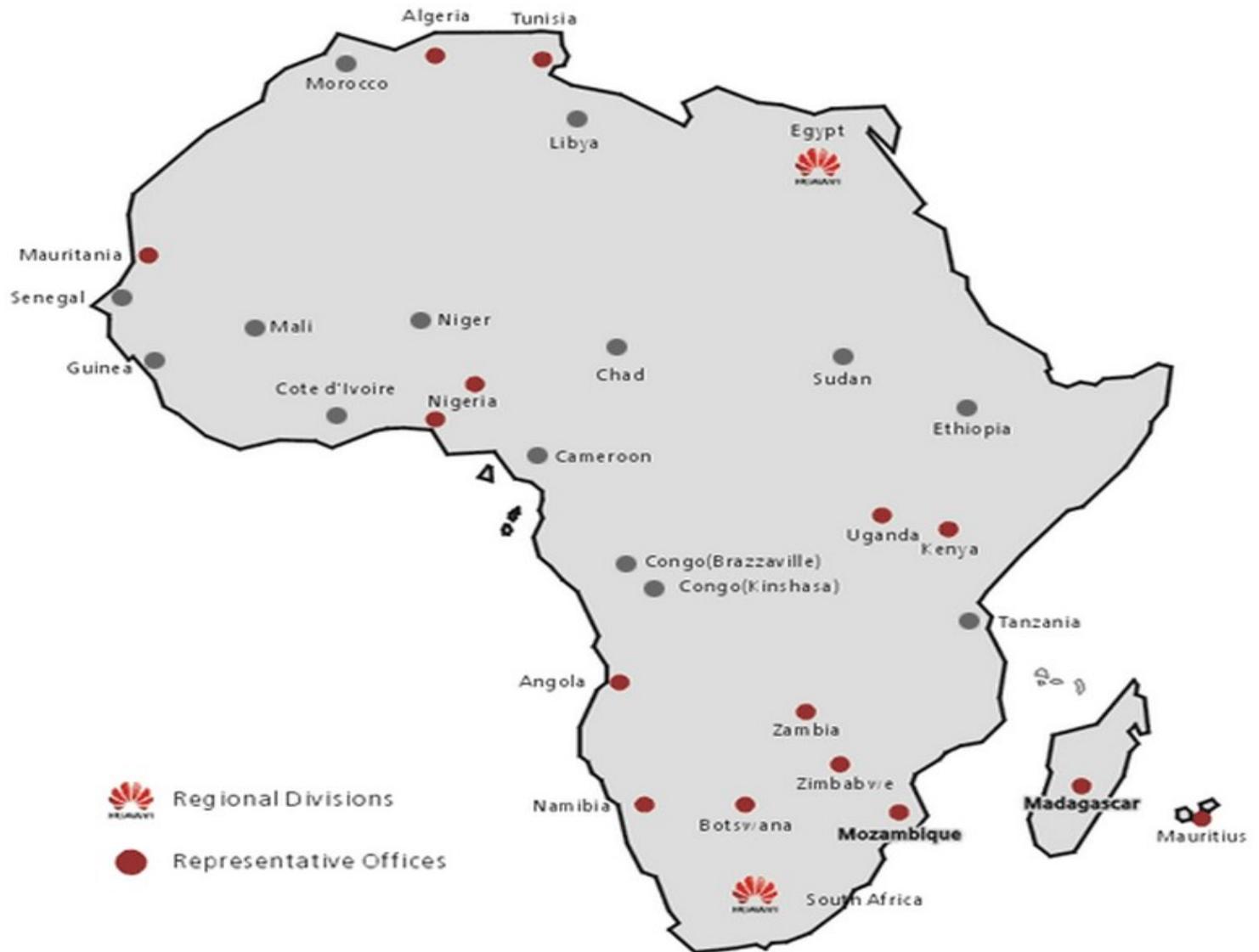
Collective Security Treaty Organization (CSTO) announced that it will start controlling social networks to avoid a repeat of mass riots like in Tunisia and Egypt.

Sources in the organization, which includes Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, say that “there is no talk about censorship or

- CSTO\* member states expected to sign the “*List of steps aimed at securing the cyberspace of the member states*”
- CSTO’s Secretary General, Nikolay Bordyuzha: the point of the document “is to prevent the usage of modern information technologies for destabilization of the situation in the CSTO states...The work on information counteraction is one of the priorities of the CSTO's activity.”

\* CSTO = Collective Security Treaty Organization (Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan)

# Huawei in Africa



# China's “economic” aid

## **China to grant Moldova 9.5 million dollars for economic, technical development**

Chisinau, December 16. /MOLDPRES/. Moldovan Prime Minister Vlad Filat and Chinese Ambassador to Moldova, Fang Li today gave a joint news briefing, after the ceremony of signing an agreement on economic and technical cooperation between the Moldovan and Chinese governments, the government's communication and press relations department has said.

"The given assistance supplements our efforts streamlined towards economic growth and decent living standards for our citizens. I would like to give assurances that as soon as possible, we will come out with concrete draft projects due to be implemented within this financial assistance," Filat said.

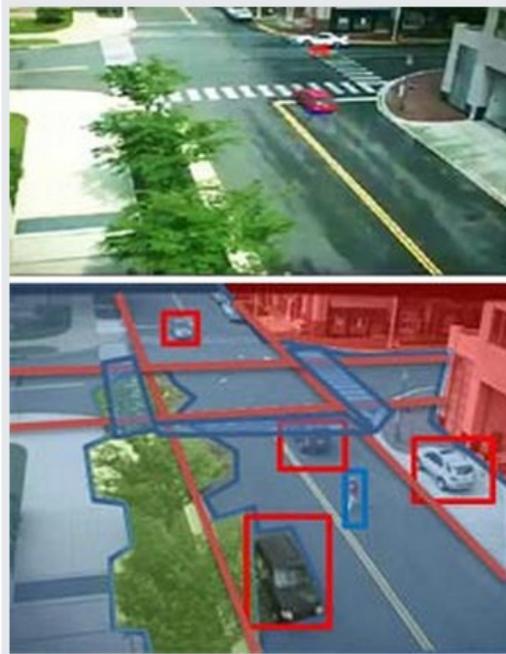
The prime minister thanked the Chinese side for the support given to Moldova through the ongoing projects in the fields of medical equipment, **video surveillance systems** for road traffic in Chisinau municipality, computers and internet connection in Moldovan student hostels.

# China-Belarus: video surveillance

**Huawei's local subsidiary:** "video surveillance system with intelligent analysis...can be used for traffic management, long-distance education and local security"

**Belarusian government:** the system "can be used for monitoring and protecting town centers, industrial plants or power and transport facilities, as well as important strategic assets, such as railway stations, airports or the state border of Belarus."

# Image to Text; Lotus Hill Institute



**Picture this:** The objects in a surveillance footage scene (top) are annotated by computer vision software (below).  
Song-Chun Zhu/UCLA

COMPUTING

## Surveillance Software Knows What a Camera Sees

*Software offers a running commentary to ease video searching and analysis.*

TUESDAY, JUNE 1, 2010 | BY TOM SIMONITE

Audio »

A prototype computer vision system can generate a live text description of what's happening in a feed from a surveillance camera. Although not yet ready for commercial use, the system demonstrates how software could make it easier to skim or search through video or image collections. It was developed by researchers at the University of California, Los Angeles, in collaboration with ObjectVideo of Reston, VA.

"You can see from the existence of YouTube and all the other growing sources of video around us that being able to search video is a major problem," says [Song-Chun Zhu](#), lead researcher and professor of statistics and computer science at UCLA.

"Almost all search for images or video is still done using the surrounding text," he says. Zhu and UCLA colleagues Benjamin Yao and Haifeng Gong developed a new system, called I2T (Image to Text), which is intended to change that.

# Thwarting the Advance

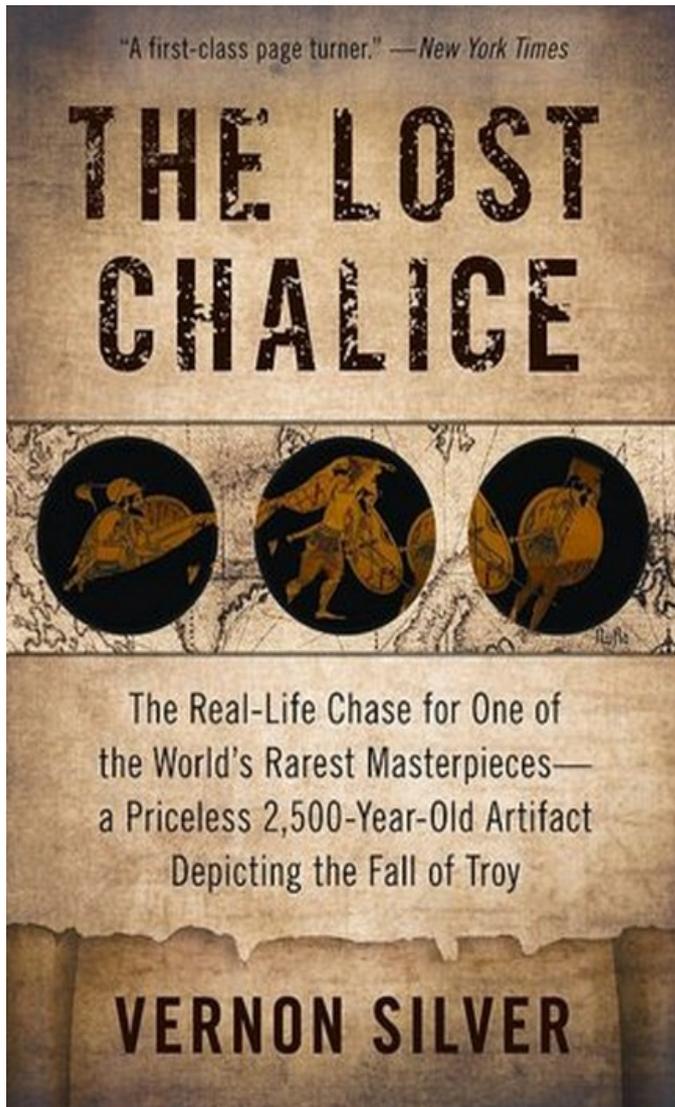
- \* Technologies for automated facial recognition, video analysis and some data-mining tasks are far from perfect and require huge academic expertise
- \* Both companies & governments are eager to pay up
- \* Need to raise awareness & costs in academia (e.g. making sure institutional review boards take the geopolitical implications of these projects seriously)

### **III. What can be done by activists?**

# Beyond Sanctions

It's time to turn the tables and engage in some surveillance of the surveillance industry

# Great fun for investigative journalists



**Bloomberg**

Our Company | Professional | Anywhere

Visit Your Queue



QUICK

NEWS

VIEW

MARKETS

PERSONAL FINANCE

SUSTAINABILITY

TV

RADIO

Related News: [Middle East](#)

Want to save this for later? [Add it to your Queue!](#)

## HP Computers Underpin Syria Surveillance

By [Vernon Silver](#) · Nov 18, 2011 7:07 PM GMT+0300

ADD TO QUEUE

Recommend 22

Tweet 234

Share 17

+1 2

More

Print

Email

[Hewlett-Packard Co. \(HPQ\)](#) equipment worth more than \$500,000 has been installed in computer rooms in Syria, underpinning a surveillance system being built to monitor e-mails and Internet use, according to documents from the deal and a person familiar with the installation.

The equipment, by Palo Alto, California-based Hewlett-Packard

# Investigations on the Cheap

## LOBBYING TRACKER

SHARE FEEDBACK

McDermott, Will & Emery for Blue Coat Systems, Inc.

**Specific issue:** Issues relating to export controls.

### Lobbyists:

Eynon, Edward (covered positions: Dep COS Cong.Shadegg; Coun:Cong.Gallegly;OIC;H GovRefOvrst; 2000-02: Deputy Chief of Staff, Rep. Shadegg; 1998-99: )

Ransom, David (covered positions: 2007-08: Sr Communications and Policy Advisor, House )

Ryan, Stephen M (covered positions: 1987-91: Gen Counsel, Govt Affairs Comm, US Senate; 1986: )

Clerk of the House of Representatives  
Legislative Resource Center  
B-106 Cannon Building  
Washington, DC 20515

<http://lobbyingdisclosure.house.gov>

Secretary of the Senate  
Office of Public Records  
232 Hart Building  
Washington, DC 20510

<http://www.senate.gov/lobby>

## LOBBYING REGISTRATION

Lobbying Disclosure Act of 1995 (Section 4)

**Check One:**  New Registrant  New Client for Existing Registrant  Amendment

1. Effective Date of Registration 10/27/2011

2. House Identification 31445

Senate Identification 24338

# LOBBYING REGISTRATION

Lobbying Disclosure Act of 1995 (Section 4)

**Check One:**  New Registrant  New Client for Existing Registrant  Amendment

1. Effective Date of Registration 10/27/2011

2. House Identification 31445

Senate Identification 24338

**REGISTRANT**  Organization/Lobbying Firm  Self Employed Individual

3. Registrant McDermott Will & Emery LLP

Address 600 13th Street NW Address2 \_\_\_\_\_  
City Washington State DC Zip 20005 - Country USA

4. Principal place of business (if different than line 3)

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_ - Country \_\_\_\_\_

5. Contact name and telephone number  International Number

Contact Stephen M. Ryan Telephone (202) 756-8333 E-mail sryan@mwe.com

6. General description of registrant's business or activities

## Law Firm

**CLIENT** *A Lobbying Firm is required to file a separate registration for each client. Organizations employing in-house lobbyists should check the box labeled "Self" and proceed to line 10.*  Self

7. Client name Blue Coat Systems, Inc.

Address 420 North Mary Avenue  
City Sunnyvale State CA Zip 94085 - Country USA

8. Principal place of business (if different than line 7)

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_ - Country \_\_\_\_\_

9. General description of client's business or activities

corporate network security and management

## LOBBYISTS

10. Name of each individual who has acted or is expected to act as a lobbyist for the client identified on line 7. If any person listed in this section has served as a "covered executive branch official" or "covered legislative branch official" within twenty years of first acting as a lobbyist for the client, *state the executive and/or legislative position(s) in which the person served.*

Name				Covered Official Position (if applicable)
First	Last		Suffix	
Stephen M.	Ryan			1987-91: Gen Counsel, Govt Affairs Comm, US Senate; 1986:
Stephen M.	Ryan			Asst US Attorney, DC; 1984-86: Deputy Counsel, President's
Stephen M.	Ryan			Commission on Organized Crime.
Edward	Eynon			2000-02: Deputy Chief of Staff, Rep. Shadegg; 1998-99:
Edward	Eynon			Counsel, Rep. Gallegly; 1997-98: Investigative Counsel,

# Telecomix's Blue Cabinet

[page](#)[discussion](#)[view source](#)[history](#)

## Blue cabinet

Blue Cabinet is a working project to document vendors and manufacturers of surveillance equipment that are used in dictatorships and democracies around the internet.

The purpose of this page is to create an overview and to share resources between Telecomix and other projects out there that have the same goal as us; *to name, shame and expose* those who profit on selling the surveillance equipment that enables the intimidation, harassment and killing of innocent people.

Insert information about companies below. Separate facts and suspicions carefully. If the information contains extensive information as basic research, consider creating a new and separate page for that.

**Please note:** Keep off-topic information such as ownership, persons, basic research and evidence material in designated pages, to avoid making this overview page bloated. It is very easy to create and link to a new page.

**Please note 2:** Limit entries to equipment that is specifically designated to either *surveillance* or *censorship*. Generic infrastructure is not relevant here, only technology which is dedicated to harmful interception.

### Contents [\[hide\]](#)

#### 1 List of companies

##### 1.1 ABILITY (Israel)

###### 1.1.1 See also

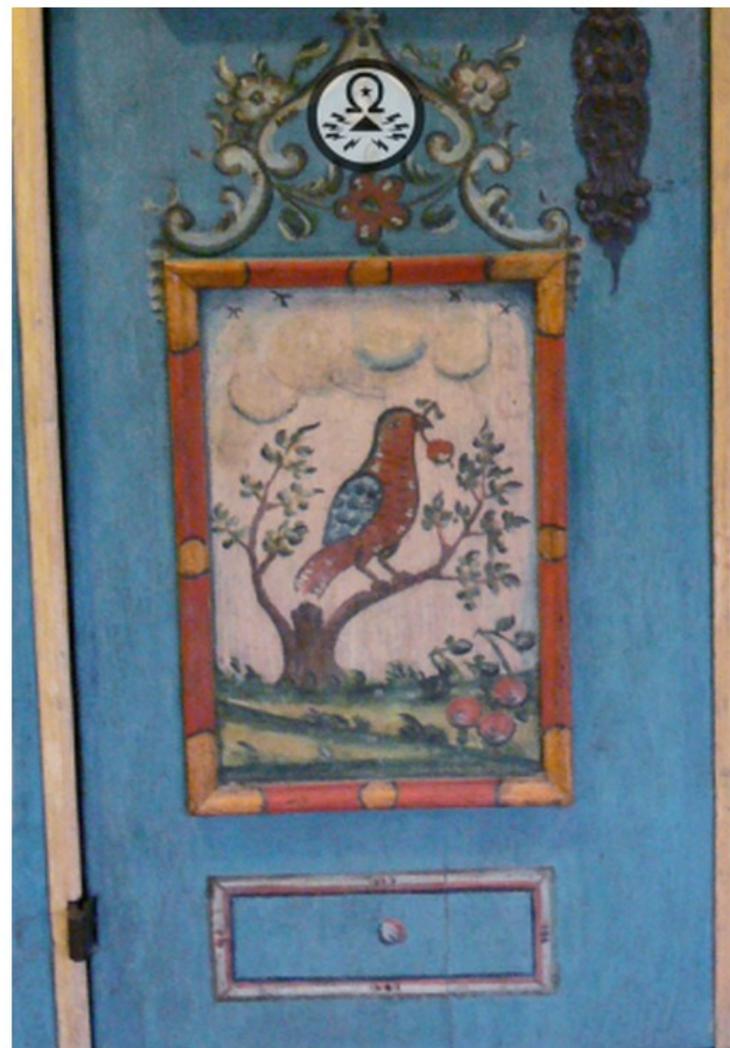
###### 1.1.2 Reports

##### 1.2 Amesys/Bull (France)

###### 1.2.1 See also

###### 1.2.2 Reports

##### 1.3 AREA S.p.A. (Italy)



# Area SpA: power of national media

**CORRIERE DELLA SERA** *it* Milano/Cronaca

Home **CorriereTV** Cronaca | Politica | Arte e cultura | Cinema e teatro | Concerti e locali | Bambini | Agenda

» Corriere Della Sera > Milano > Cronaca > «E' Vero, Lavoro Per «Spiare» La Siria. Ma Da Due Mesi Il Pro...

Share 8 Tweet 3 Consiglia 31

L'INTERVISTA PARLA IL PRESIDENTE DELL'AZIENDA DI VIZZOLA TICINO

## «E' vero, lavoro per «spiare» la Siria. Ma da due mesi il progetto è fermo»

*L'azienda prepara un sistema di intercettazione del traffico Internet per conto del regime di Assad*



**Attivisti antigovernativi siriani protestano a Vizzola Ticino (Milestone Media)**

**VIZZOLA TICINO (Va)** - Dottor Formenti, allora è vero o no che lavorate per la Siria? «In questi giorni sono uscite sul nostro conto cose vere e altre molto meno. Però è così: abbiamo in corso un contratto con un partner locale». Andrea Formenti, presidente di Area spa, la software house di Vizzola Ticino (Varese) finita al centro di un caso perché starebbe fornendo un sistema di intercettazione del traffico internet per conto del regime di Bashar Assad, rompe il silenzio. Senza sottrarsi, per quanto la situazione lo consente, ai chiarimenti.

**Partiamo allora dal principio: come è nata la collaborazione con la Siria?**

«Semplicemente abbiamo vinto una gara d'appalto internazionale; era il 2008. Assieme alla Area

# Investors can be swayed as well..

## Weak Commitment to Human Rights Factors into Boston Common's Decision to Divest of Cisco Systems

Manipulative Vote Tallying Further Isolates Cisco

Submitted by: **Boston Common Asset Management**

Categories: **Business Ethics, Human Rights**

Posted: Jan 11, 2011 – 08:00 AM EST



**BOSTON COMMON**  
ASSET MANAGEMENT, LLC

---

BOSTON, Jan. 11 /CSRwire/ - Boston Common Asset Management, LLC has divested of its holdings in Cisco Systems, Inc. stock (NYSE: CSCO) due in part to the company's weak human rights risk management and poor response to investor concerns. Cisco's deceptive announcement of vote results on proxy items at the 2010 annual shareholder meeting has raised further alarm about the company's commitment to transparency.

Since 2005 Boston Common has led a growing coalition of investors, representing over 20 million Cisco shares, in asking Cisco management to ensure its products and services do not stifle human rights. Cisco has testified before federal law makers twice since 2006 over questions on its human rights record, including its marketing of equipment to the Chinese Ministry of Public Security.

# Investigating individual companies



[OUR SOLUTIONS](#) | [OUR TECHNOLOGY](#) | [SUCCESS STORIES](#) | [IN THE NEWS](#) | [ABOUT US](#)

[Home](#) > [About Us](#) > Investors

## Investors

[Draper Fisher Jurvetson](#) | [Palisades Ventures](#) | [ePlanet Ventures](#)

Polaris Wireless is a private venture capital funded company with ownership held by outside investors and the company management and employees. The principal outside investors are Silicon Valley-based Draper Fisher Jurvetson (and Draper Richards) and Los Angeles-based Palisades Ventures.

### Draper Fisher Jurvetson



Draper Fisher Jurvetson is the only venture capital firm with global presence through a network of partner funds, with offices in more than 33 cities around the world and approximately \$5.5 billion in capital commitments. DFJ's mission is to identify, serve, and provide capital for extraordinary entrepreneurs anywhere who are determined to change the world. Over the past twenty years, DFJ has been proud to back approximately 400 companies across many sectors including such industry changing catalysts as Hotmail (acquired by MSFT), Baidu (BIDU), Skype (acquired by EBAY), United Online (UNTD), Overture (acquired by YHOO), Athenahealth (ATHN), EnerNOC (ENOC), Interwoven (IWOV), Four11 (acquired by YHOO), Parametric (PMTC), and Digidesign (acquired by AVID).

GeoWorld: Who are the major customers for this type of product, and what are some of their uses?

**Polaris: [Our technology] has been deployed by government agencies in the Middle East/Africa and Asia-Pacific regions for use in their anti-crime and anti-terrorism surveillance efforts.**

# Polaris Wireless in their own words

“...customers can create a **custom geo-fenced area** and locate all subscribers in it, as well as receive alerts when designated targets **enter or exit the geo-fence**.

The geo-fenced area can be identified in real time or at a specified time in the past, enabling government agencies to perform critical post-event analytics to discover...which subscribers were in the vicinity of a busy downtown intersection during the hours before a terrorist event occurred.

...Polaris Wireless plans to expand the Altus application suite with the ability to **assess risks** based on multiple inputs, including user identity, call logs, and social data.”

# 2011: A very good year for Polaris

01 Nov 2011

## Polaris Wireless Announces Expansion in MEA Region with Multi-Million Dollar Contract

Text size  

*Deal Expands Global Footprint of OmniLocate High-Accuracy Wireless Location Platform and Altus Solution for Law Enforcement & Intelligence Agencies*

MOUNTAIN VIEW, Calif. & DUBAI, United Arab Emirates- Nov. 1, 2011 -(BUSINESS WIRE/ME NewsWire)-- Polaris Wireless, the global leader in high-accuracy, software-based wireless location solutions, today announced a significant customer contract, for a multi-million dollar deployment of the Polaris Wireless Altus and OmniLocate location surveillance product suite. The deal represents a major increase in Polaris Wireless' business in the MEA region, directed out of the company's regional headquarters in Dubai. This is the latest deployment of the company's high-accuracy wireless location surveillance solution in an area increasingly vital to the global efforts against crime and terrorism. Polaris Wireless high-accuracy location solutions are also deployed in North America and the Asia-Pacific region.

## Polaris Wireless Doubles Manpower in India from Present 55

2011-12-03 03:58:42, India

Polaris Wireless, a global provider of high accuracy, software-based wireless location solutions to wireless operators, law enforcement / government agencies and location-based application companies, is planning to double its manpower in India from the present 55 people.

The company has development centers in Bangalore and Nagpur. The US-based company is aiming to achieve \$100 million revenue next year. Polaris Wireless has more than 120 people globally.

"We are planning to increase our investment in India. We will double our Indian manpower next year. We hope to work with all leading operators in India to assist them in their wireless location projects," said Manilo Allegra, president and CEO of [Polaris Wireless](#).

# These companies have allies...

## The Telegraph

### British firm with links to William Hague sells 'protester-tracking' product to Iran

A British technology firm with links to William Hague, the Foreign Secretary, has sold a product to Iran which could be used to track down protesters.

By **Holly Watt, Claire Newell and Helia Ebrahimi**

7:15AM GMT 07 Nov 2011

---

Creativity Software sold the product to the regime despite concerns that it has been used to round up activists communicating with their mobile phones.

*“MMC Ventures is a major shareholder in Creativity Software. The chief executive of MMC is Bruce Macfarlane and the chairman is Alan Morgan, both of whom paid part of the salary of Chloe Dalton, a researcher for Mr Hague between 2006 and 2009. They contributed £25,000 to Mr Hague’s private office.”*

# ...and balls



creativity software

Creativity Software Ltd  
River Reach,  
31-35 High St  
Kingston-Upon-Thames  
Surrey KT1 1LF

**Statement 10 November 2011**

Creativity Software is proud to be a supplier of world class technology to MTN, in Iran and other countries. MTN is a company with the vision of being the leading telecommunications provider in emerging markets, with an avowed mission to speed up the progress of the emerging world by enriching the lives of the people within it.

# **IV. Linking Spread of Surveillance Gear & Domestic Surveillance Debate in Democracies**

# Web Surveillance Software and Jobs

[Article](#)[Comments \(2\)](#)

Email



Print

Save



Like

53



1



Tweet

533



The article "[Document Trove Exposes Surveillance Methods](#)" (page one, Nov. 19) will have a negative effect on job creation in the U.S. as attention of this kind makes U.S. manufacturers gun shy about developing, and eventually exporting, anything that can remotely be used to support government surveillance.

Based on our work with customers from around the globe, we expect that most countries outside the U.S. and Western Europe will begin to place intercept mandates on social networks, especially following the Arab Spring. This would give U.S. companies an opportunity to develop such tools and thus create jobs.

We are concerned that the article and others like it contribute to an atmosphere where Congress isn't likely to pass an updated lawful-interception law. The law would require social-networking companies to deploy special features to support law enforcement. Without the update, the opportunity for U.S. companies to develop and launch intercept products domestically for eventual export will be greatly curtailed.

Additionally, in some countries U.S. companies are already refusing to provide intercept support and are banned from doing business. But Chinese equivalents, with lawful-intercept features, crop up in their absence. Like it or not, many countries will adopt the Chinese model, leaving U.S. companies and job growth behind.

**Tatiana Lucas**

*World Program Director*

*Intelligence Support Systems*

*McLean, Va.*

# Translation

- I. If dictators need help in suppressing democratic uprisings, we are to help
- II. Oh no: Our dictator-helping jobs are going to China!
- III. This market has one major driver – needs of US law enforcement

# “We are here to help”: need to attack & ridicule their arguments

**Jerry Lucas, ISS's founder** : “This technology is absolutely vital for civilization. You can't have a situation where bad guys can communicate and you bar interception.”

**Lucas**: “When you're selling to a government, you lose control of what the government is going to do with it. It's like selling guns to people. Some are going to defend themselves. Some are going to commit crimes.”

**Lucas**: “not my job to determine who's a bad country and who's a good country. That's not our business, we're not politicians ... we're a for-profit company. Our business is bringing governments together who want to buy this technology.”

**Klaus Mochalski**, co-founder of ipoque: “It's like a knife. You can always cut vegetables but you can also kill your neighbor.”

“China will take our jobs!” → situation is okay

## Huawei Restricts Business in Iran, No Longer Seeks New Customers

By Michael Kan, IDG News

Huawei Technologies will limit its business activities in Iran and no longer seek new customers there, it said Friday, after an October report said the Chinese company was building a surveillance system in the country to help police track people's locations via their mobile phones.



### SIMILAR ARTICLES:

[Huawei Aims to Be Major Player in U.S. Smartphone Market](#)

[Huawei Sues Motorola to Protect Intellectual Property](#)

[Nokia Siemens Scales Down Presence in Iran](#)

[Hands-On With the Huawei Ascend II for Cricket](#)

"Due to the increasingly complex situation in Iran, Huawei will voluntarily restrict its business development there,"

it said in a brief [online statement](#). The move includes limiting its business activities with current customers, although Huawei will continue to provide services to the existing communication networks it was contracted to build.

Huawei will "voluntarily restrict its business development there by no longer seeking new customers and limiting its business activities with existing customers...For communications networks that have been delivered or are under delivery to customers, Huawei will continue to provide necessary services to ensure communications for Iran's citizens"

# Link to domestic surveillance most serious & undertheorized

According to *The Washington Post*, one of ISS fairs was attended by “representatives from 35 [US govt] agencies, including the FBI, the Secret Service and every branch of the military, along with the IRS, the Agriculture Department and the Interior Department's Fish and Wildlife Service.”

# FBI's “Going Dark” “problem”

EFF's FOIA request: “a five-pronged Going Dark program that includes extending existing laws and seeking new federal funding to bolster lawful intercept capabilities. Going Dark has been an FBI initiative since at least 2006 and has involved writing checks to consultants at RAND Corporation and Booz, Allen and Hamilton.”

Defining the problem: “As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage —evidence that a court has authorized the government to collect.”

# The rationale behind “Going Dark”

“...We are focusing on the interception of electronic communications and related data in real or near-real time. Without the ability to collect these communications in real or near-real time, investigators will remain several steps behind and left unable to act quickly to disrupt threats to public safety or gather key evidence that will allow us to dismantle...”

“The government understands that [for sophisticated criminals] it must develop individually tailored solutions. However, individually tailored solutions have to be the exception and not the rule.”

*From the testimony of Valerie Caproni,  
General Counsel for FBI, Statement Before the House Judiciary  
Committee, Subcommittee on Crime, Terrorism, and Homeland  
Security Washington, D.C. February 17, 2011*

# Tools vs CALEA 2 debate before “spy files”

“... if the FBI obtains a probable cause-based court order before installing tools like CIPAV, complies with the minimization requirements in federal wiretapping law by limiting the time and scope of surveillance, and removes the device once surveillance concludes, the use of these types of targeted tools for Internet surveillance would be a much more narrowly tailored solution to the FBI’s purported problems than the proposal to undermine every Internet user's privacy and security by expanding CALEA”

*Jennifer Lynch, staff attorney EFF, on EFF's blog April 2011*

# Tools vs CALEA 2 debate now

EFF's argument needs to be revised; the deployment of such tools – even if done perfectly well in Western democracies – affects the rest of the world, as such tools make their way to the secondary market.

# Prediction for the future

Left unchallenged, FBI would get the best of possible worlds: individually tailored solutions (that industry already exists) and legally-required backdoors

The international implications of CALEA-2: other govts will obtain access to the backdoors

In any event, FBI has an “alibi”, for it can now say that activists preferred individual tools to CALEA-2

# Opportunities...

\* This debate about dictators using surveillance tools is an opportunity to criticize the expansion of domestic surveillance and the strategy of FBI and its European partners. It's for sure an argument against CALEA -2

\* Media coverage should focus more on the domestic part and take a macro-level view; press articles need to link all of this to CALEA and beyond

**V. Most important bit: getting  
foreign policy right**

# US State Dept & Cisco: Context...

## Human rights group sues Cisco in China

ANI Sep 7, 2011, 11.49am IST

**Tags:** [Tracking](#) | [Software](#) | [human rights group](#) | [Cisco](#)

WASHINGTON: A human rights group has sued technology giant, Cisco for aiding the tracking and torture of Chinese citizens through its technology.

Washington-based Human Rights Law Foundation alleged that Cisco developed an anti-virus software to help the Chinese Government monitor and jail the banned [Falun Gong](#) members as a part of the "Golden Shield Project", the [Sydney Morning Herald](#) reports.



The Golden Shield Project was undertaken by the Chinese government to censor references to politically sensitive topics such as Tiananmen Square, and the Middle East revolution.



0      0      

 Tweet     Recommend     Submit

# Realities of US foreign policy - I

MIDDLE EAST NEWS | JUNE 15, 2010

## U.S. Deploys Tech Firms to Win Syrian Allies

Article

Stock Quotes

Comments (22)



101



0



10



By JAY SOLOMON



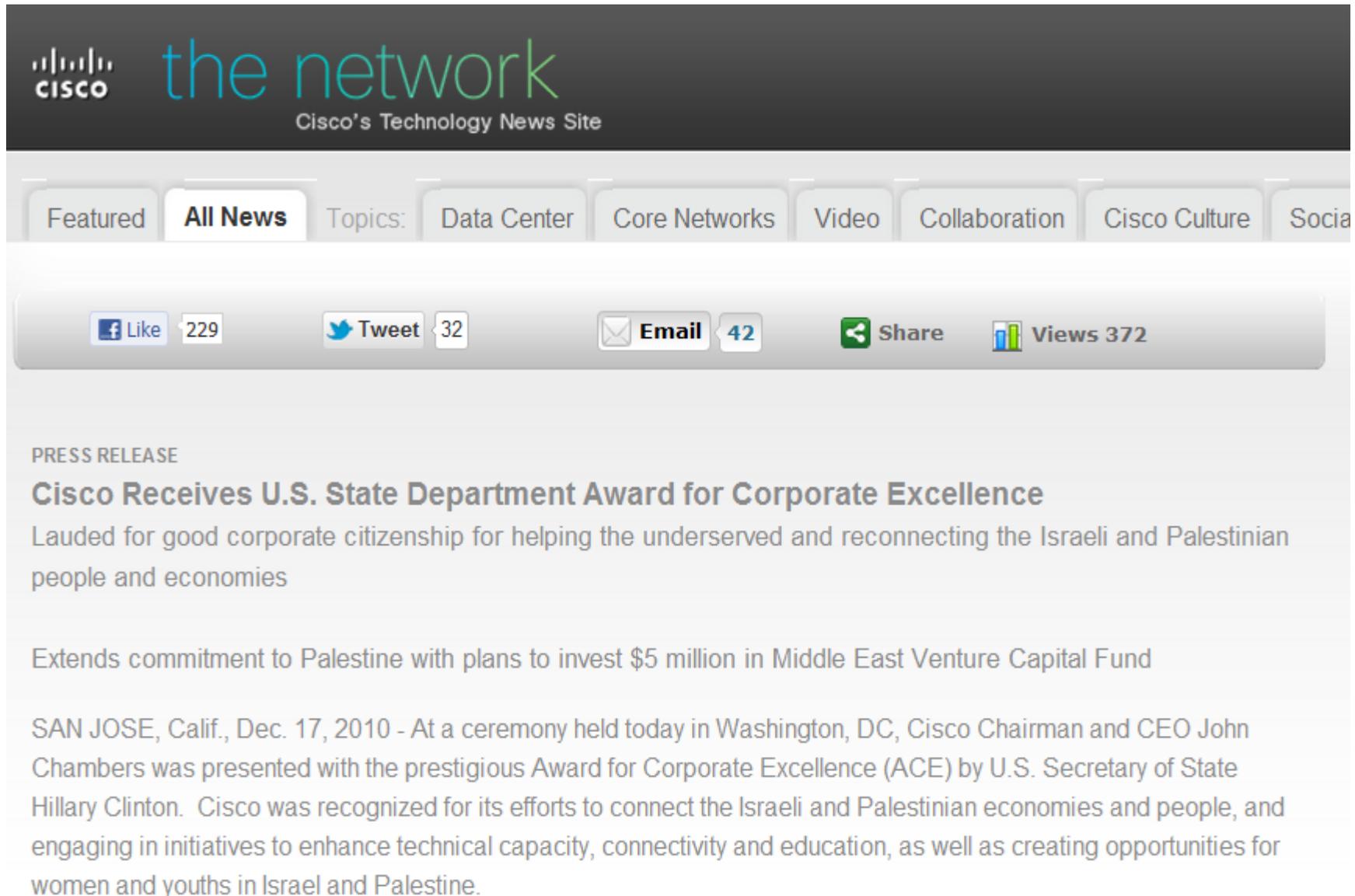
Associated Press

Israeli tanks in the Golan Heights in September, 2007 after the bombing of an alleged Syrian nuclear site.

WASHINGTON—The State Department has dispatched a high-level diplomatic and trade mission to Syria, according to senior U.S. officials, marking the latest bid by the Obama administration to woo President Bashar al-Assad away from his strategic alliance with Iran.

The U.S. delegation comprises senior executives from some of America's top technology companies, including [Microsoft Corp.](#), [Dell Inc.](#), [Cisco Systems Inc.](#) and [Symantec Corp.](#), according to the U.S. officials. All these companies' businesses in Syria are constrained by U.S. sanctions.

# Realities of US foreign policy - II



**CISCO** the network  
Cisco's Technology News Site

Featured **All News** Topics: Data Center Core Networks Video Collaboration Cisco Culture Social

 Like 229  Tweet 32  Email 42  Share  Views 372

PRESS RELEASE

## Cisco Receives U.S. State Department Award for Corporate Excellence

Lauded for good corporate citizenship for helping the underserved and reconnecting the Israeli and Palestinian people and economies

Extends commitment to Palestine with plans to invest \$5 million in Middle East Venture Capital Fund

SAN JOSE, Calif., Dec. 17, 2010 - At a ceremony held today in Washington, DC, Cisco Chairman and CEO John Chambers was presented with the prestigious Award for Corporate Excellence (ACE) by U.S. Secretary of State Hillary Clinton. Cisco was recognized for its efforts to connect the Israeli and Palestinian economies and people, and engaging in initiatives to enhance technical capacity, connectivity and education, as well as creating opportunities for women and youths in Israel and Palestine.

# But Europe isn't innocent either...

From ***The Wall Street Journal***: “In 2007, Mr. Sarkozy welcomed Gadhafi on an official visit to France, his first in more than three decades. *The Libyan regime saw an opportunity to upgrade its surveillance capability with French technology*, according to people familiar with the matter. Amesys signed its contract with Libya that year, it said, and then in 2008 shipped its "Eagle" surveillance system and sent engineers to Libya to help set it up. The system became fully operational in 2009...”

# Foreign Policy challenges

- Iran is an easy target – few Western govts like it

- But what about Saudi Arabia\* or Bahrain\*\*?

- \* in 2010 Washington approved a \$60 billion (!) arms deal with Saudi Arabia

- \*\* A \$53 million arms sale to Bahrain is currently under consideration in the White House

# Challenges Ahead

- With cases like Bahrain or Saudi Arabia, the challenge is much deeper
- (Suppose Websense is used in Saudi Arabia – what then...?)
- Building tools or banning exports of tools won't be enough
- An opportunity for the Pirate Parties and others to develop an explicit foreign policy dimension?

Thank you!

Twitter: [@evgenymorozov](https://twitter.com/evgenymorozov)