

***Fighting Crime Now:***

***Prevention and Effective Surveillance***

*Or*

***Today's Effective Surveillance***

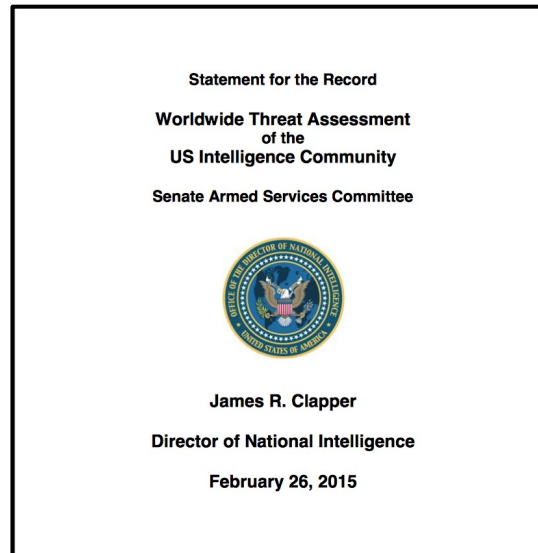
**]HackingTeam[**  
ISS World, South Africa

# Challenge of Terrorism

- Ottawa Parliament, Oct 2014
- Lindt Café, Australia, Dec 2014
- Charlie Hebdo, Jan 2015
- Italians arrest Vatican plotter, April 2015



# Transnational Organized Crime – U.S. Senate Report



“Savvy, profit-driven criminal networks traffic in drugs, persons, wildlife and weapons, corrode security and governance, undermine legitimate economic activity and the rule of law; cost economies important revenues...”

Worldwide Threat Assessment, Feb. 26, 2015

# Transnational Organized Crime – Interpol



INTERPOL

Organized criminals, acting globally, are  
**“fast exploiting technology and leaving governments and their police forces behind.”**

Interpol, April 2015

# Crime in the Digital Age

**Cyber Crime**

**Terrorism**

# Cybercrime Cost

**\$400 Billion world-wide - Ponemon**  
Institute/McAfee Study, 2014

## Direct Costs:

- Theft of Intellectual Prop
- Financial Assets

## Indirect Costs:

- Protection
- Remediation
- Reputation Damage



# Cybercrime Cost

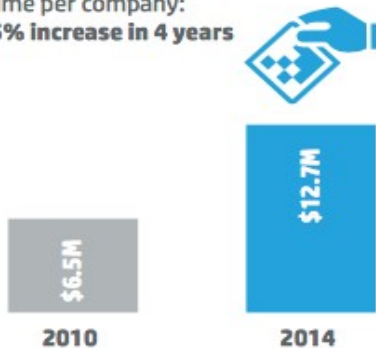
- **\$400 Billion world-wide** - Ponemon Institute/McAfee Study, 2014



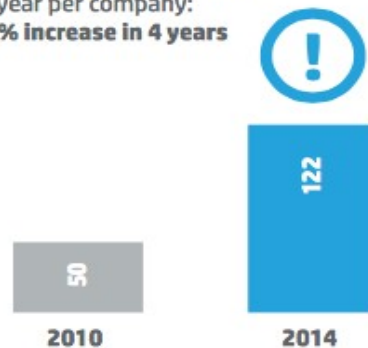
## The problem\*

Costs and incidence of attacks are high and growing.

Average cost of cyber crime per company:  
95% increase in 4 years



Number of successful attacks per year per company:  
144% increase in 4 years



Average time to resolve incidents:  
221% increase in 4 years



HP Study, 2014

# Crime in the Digital Age

**Cyber Crime**

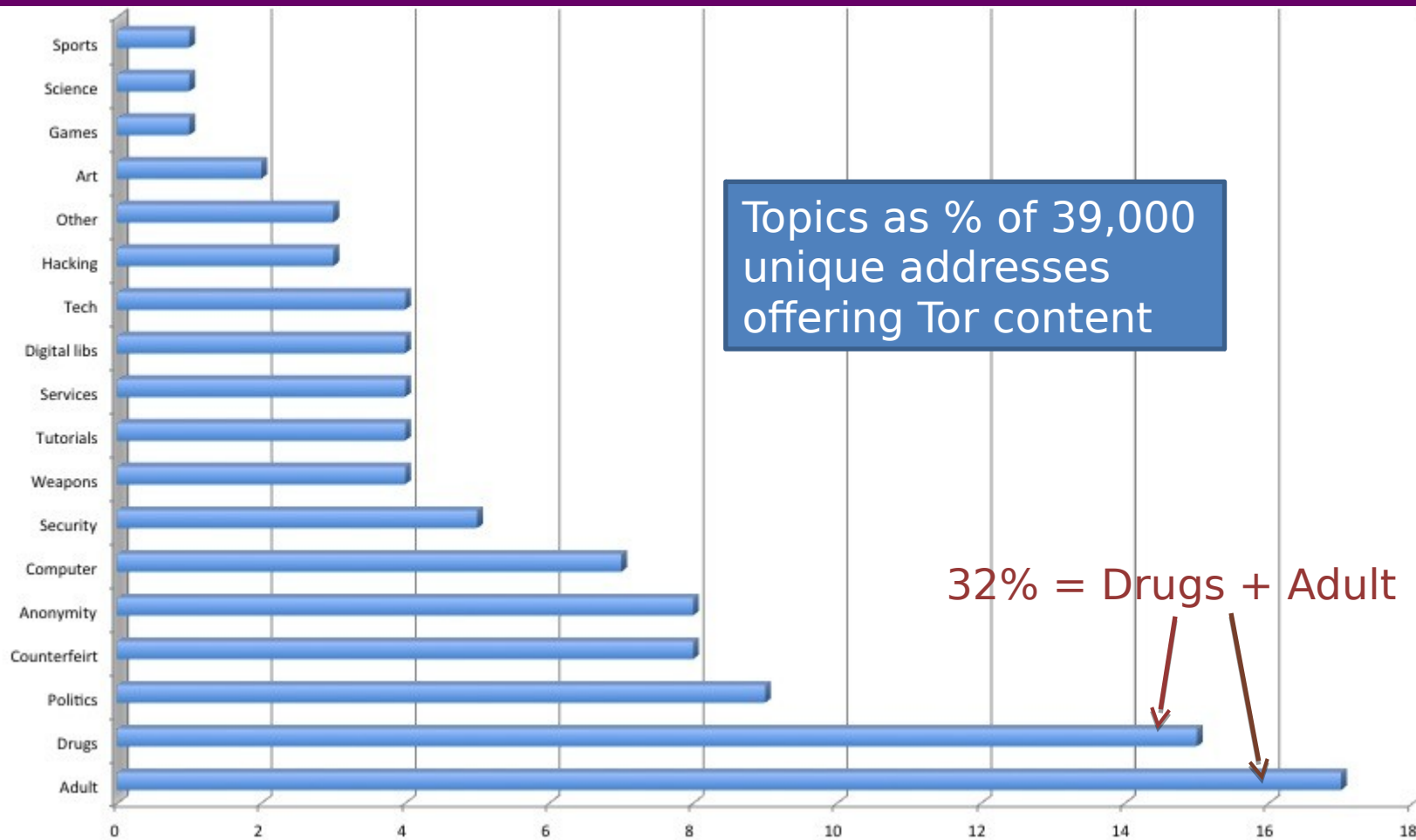
**Old Crime,  
New Tools**

**Terrorism**





# Topics discussed on Tor – 2013 study



# Silk Road's Ross Ulbricht



Convicted February,  
Sentenced to Life in  
Prison May 2015

# Dangerous Developments

- ◆ Rise of Digital Criminals
- ◆ Global Reach from the Comfort of Home
- ◆ Complete Anonymity
- ◆ Digital anonymous currency

# Evolution of Networks

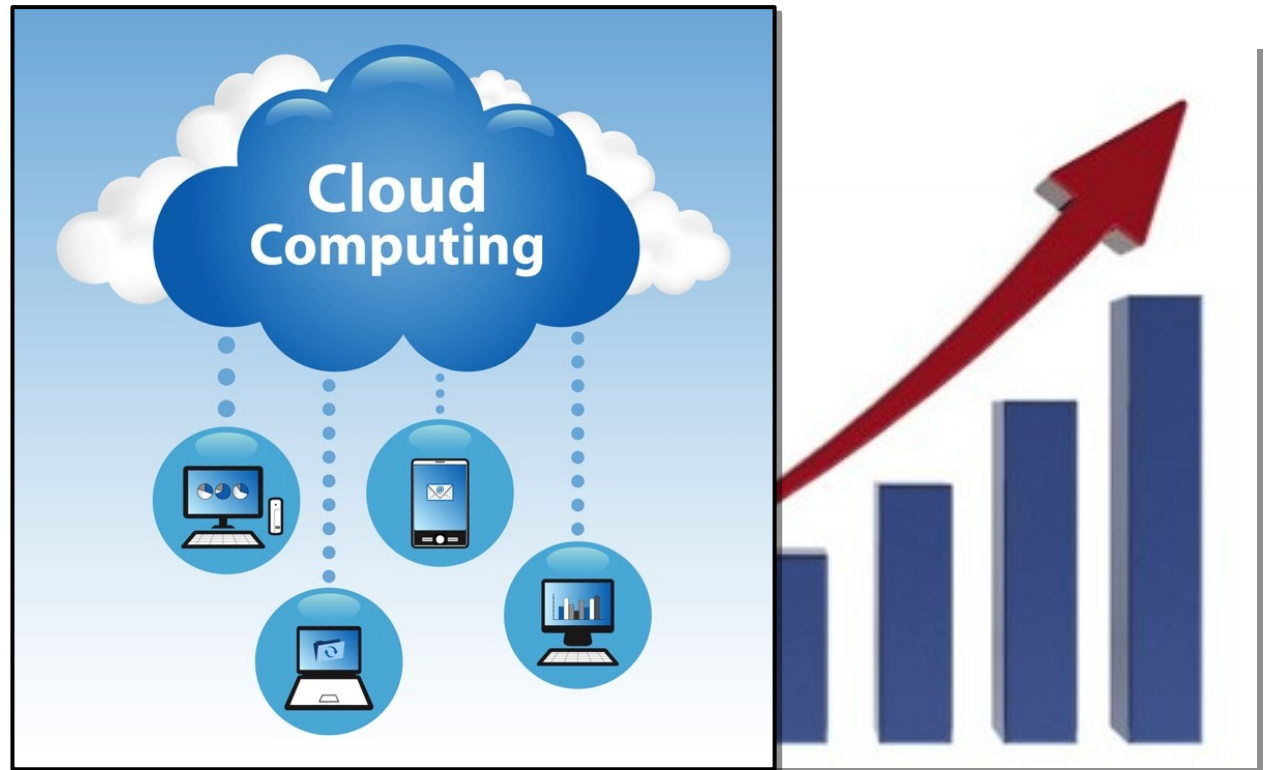




]HackingTeam[

# Cloud Adoption

More and more, data is moving to the cloud.





# Obama and Cameron on Encryption



**Obama:** Police and spies should not be locked out of encrypted smartphones and messaging apps.... Jan 16, 2015



**Cameron:** We should try to avoid the safe havens that could otherwise be created for terrorists to talk to each other.

# U.S. Federal Bureau of Investigation



The pendulum has “swung too far” against the government.

FBI Director James Comey, Oct. 16, 2014



# Britain's GCHQ



The Internet has become “command-and-control networks of choice for terrorists and criminals.”

Director Robert Hannigan, Nov. 3, 2014

# French PM Manuel Valls



“We have to focus on the Internet and social networks, which are more than ever used to recruit, organize and disseminate technical knowhow to commit terrorist acts.... We must go further.”

PM Manuel Valls, Address to French Parliament, Jan. 13, 2014

# Tim Cook, Apple



“We shouldn't give in to scare-mongering or to people who fundamentally don't understand the details...”

CEO Tim Cook, Nov. 3, 2014

Customers “...protected by end-to-end encryption across all your devices...”

Apple Website



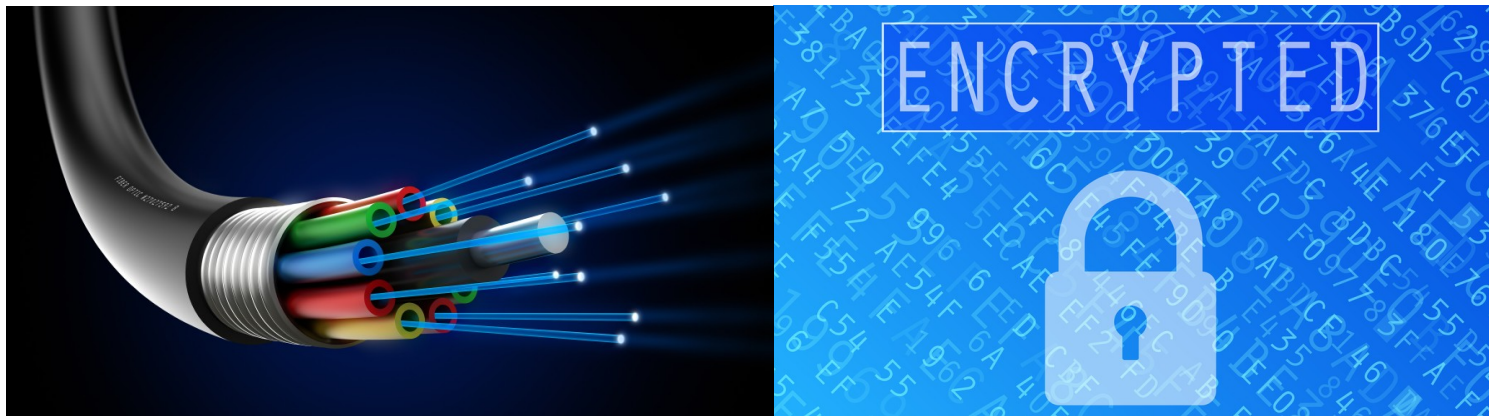
“We continue our ongoing efforts to encrypt all Google products and services.”

Google in *The Intercept*

# Impact

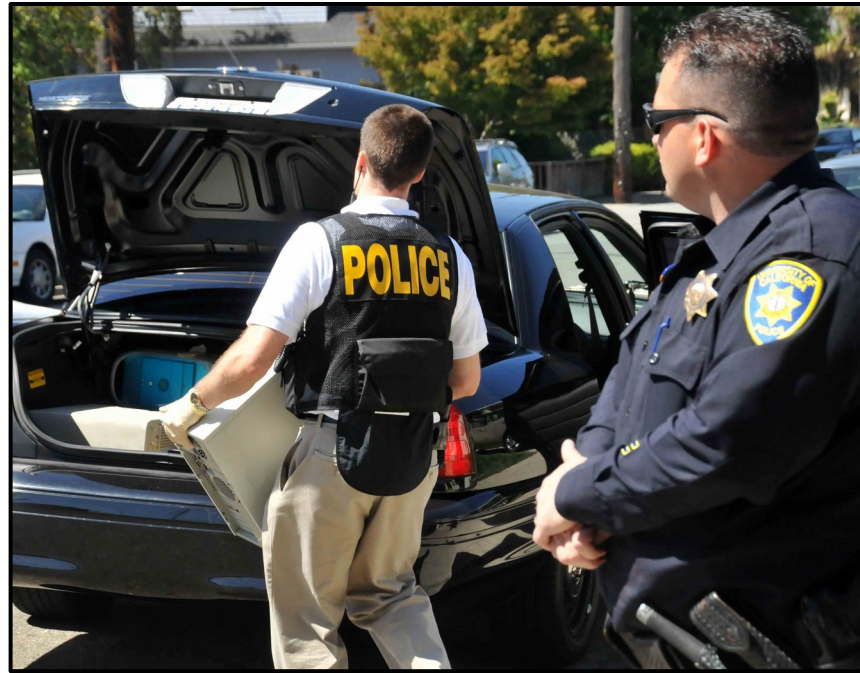
How does this change the surveillance ecosystem?

What does it all mean for Law Enforcement?



# Seizing

Not effective anymore:





# Is there a way around?

How does your suspect access the information?...



From the device...



# Is there a way around?

You want to be on the device and see information when your suspect does.



*But how can you do that?*





REMOTE CONTROL SYSTEM

GALILEO

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION



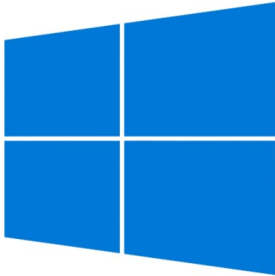
RCS infrastructure

On the device.

Bypass encryption

See what the suspect sees

Follow your suspect



]HackingTeam[

What will you see?

]HackingTeam[








# Evidence

Remote Control System

Accounting **Operations** Intelligence Dashboard Alerting <sup>1</sup> System Audit Monitor <sup>2</sup>

All operations ▶ Swordfish ▶ Jimmy Page ▶ Evidence

Open Detail Show Summary Download Evidence Relevance Add Report Edit Note Show ID Filters Presets Reset filters Translation

Acquired	Received	Type	Info	Note	Agent
2015-05-18 12:57:55	2015-05-18 12:58:54	Camera			Laptop (1)
2015-05-18 12:57:57	2015-05-18 12:58:55	Addressbook	 Name: pangoeeye@mailcatch.com	Info:	Laptop (1)
2015-05-18 12:57:57	2015-05-18 12:58:55	Addressbook	 Name: scissor@mailcatch.com	Info:	Laptop (1)
2015-05-18 12:57:57	2015-05-18 12:58:55	Addressbook	 Name: Jimmy Page	Info:	Laptop (1)
2015-05-18 13:01:44	2015-05-18 13:02:46	Keylog	Content: secret123TP!	Program: TrueCrypt.exe Window: Enter password for C:\Users\IRCS DemoDesktop\secret_op.tc	Laptop (1)
2015-05-18 13:09:45	2015-05-18 13:10:48	Chat	To: alejandro.reade jimmy.page  Program: SKYPE	Content: alejandro.reade: Here we are!	Laptop (1)
2015-05-28 13:09:52	2015-05-28 13:10:51	Call	Program: Skype   Duration: 00:00:49 From: -   To: alejandro.reade  		Laptop (1)

Showing: 49/49

demo@demo disconnected Thu, May 28 14:18:08


# Profiling

Remote Control System

AccountingOperationsIntelligenceDashboardAlertingSystemAuditMonitor

All operationsdaVinciJohn Doe

John DoeFilter data from:to:



**Born:** 10/16/1962  
**Nationality:** USA  
**Sex:** Male  
He is suspected to be a key figure of the terrorist cell.

**Accounts:**


- johndoe69
- johndoe@gmail.com
- johndoe
- johndoe@hotmail.com

**Most Contacted:**

jack.brown@gmail.com	34%
mary.smith@gmail.com	21%
uncletom	14%
bob75	12%
alice.white	12%

☒ Last Positions☐ Addresses☐ Visited Places

MapSatelliteHybridTerrain



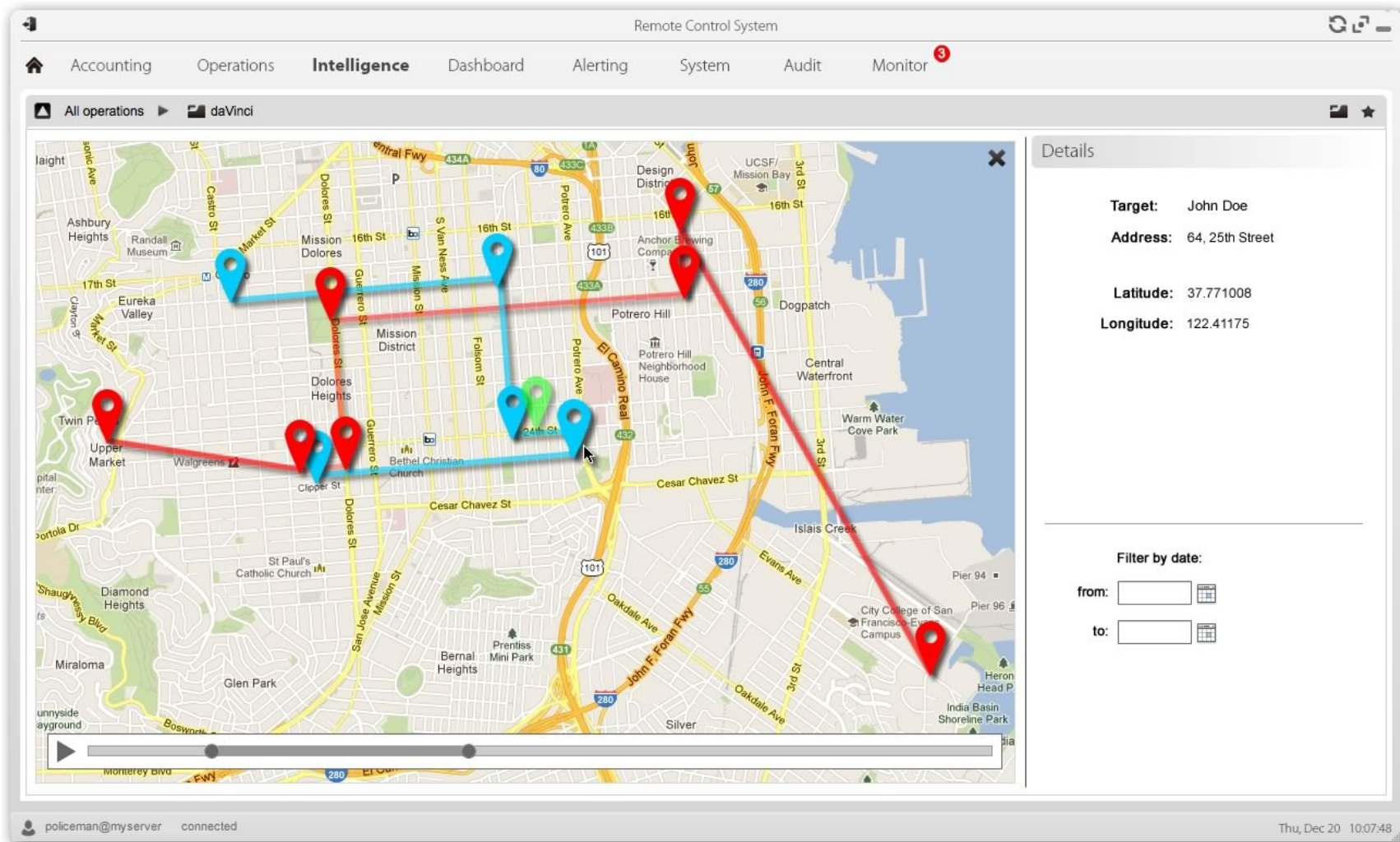
Map data ©2012 Google, Sanborn - Terms of Use

- 850 bryant Street - San Francisco, CA
- 212 12th Street - San Francisco, CA
- 340 Harrison Street - San Francisco, CA
- 15 Bernice Street - San Francisco, CA

policeman@myserver connectedThu, Dec 20 10:07:48



# Correlation





# How can I deploy my agent?

**When the target opens a document**



**Exploit Delivery  
Service**

Always up to date

**While the target browses the web**



]HackingTeam[



Send your target a SMS



QR Code

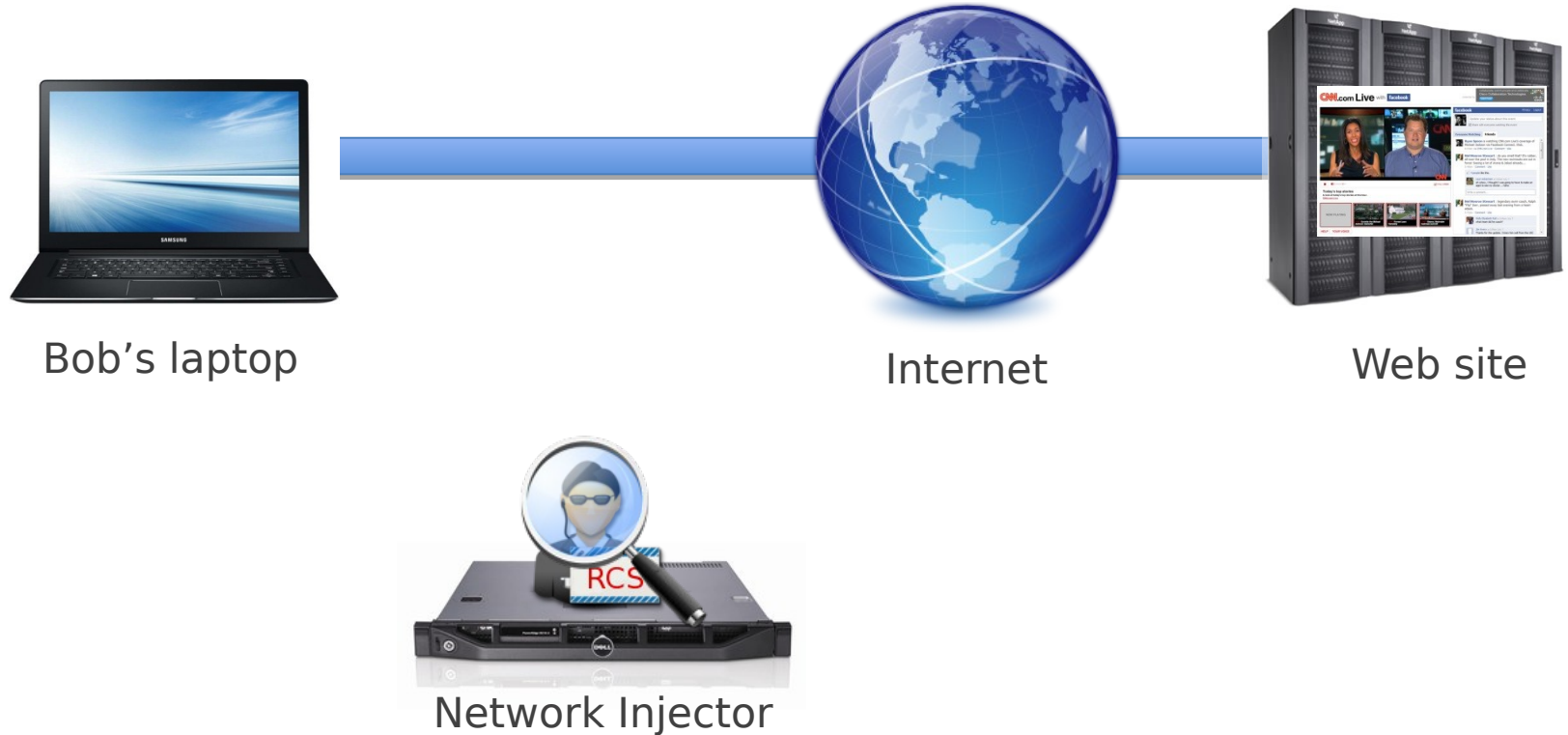


Web link

]HackingTeam[

# Inject into downloaded **applications**

## Inject into **Web** pages



**Invisible** to antiviruses.

Prevent disclosure of your presence.

500+ tests every day.

There is much more.  
Come see the live demo!

Today 15:00-16:00 Session A  
**Intruding personal devices with Remote Control  
System: Live Demo of latest attack and data  
gathering techniques**

]HackingTeam[

# Public Opinion

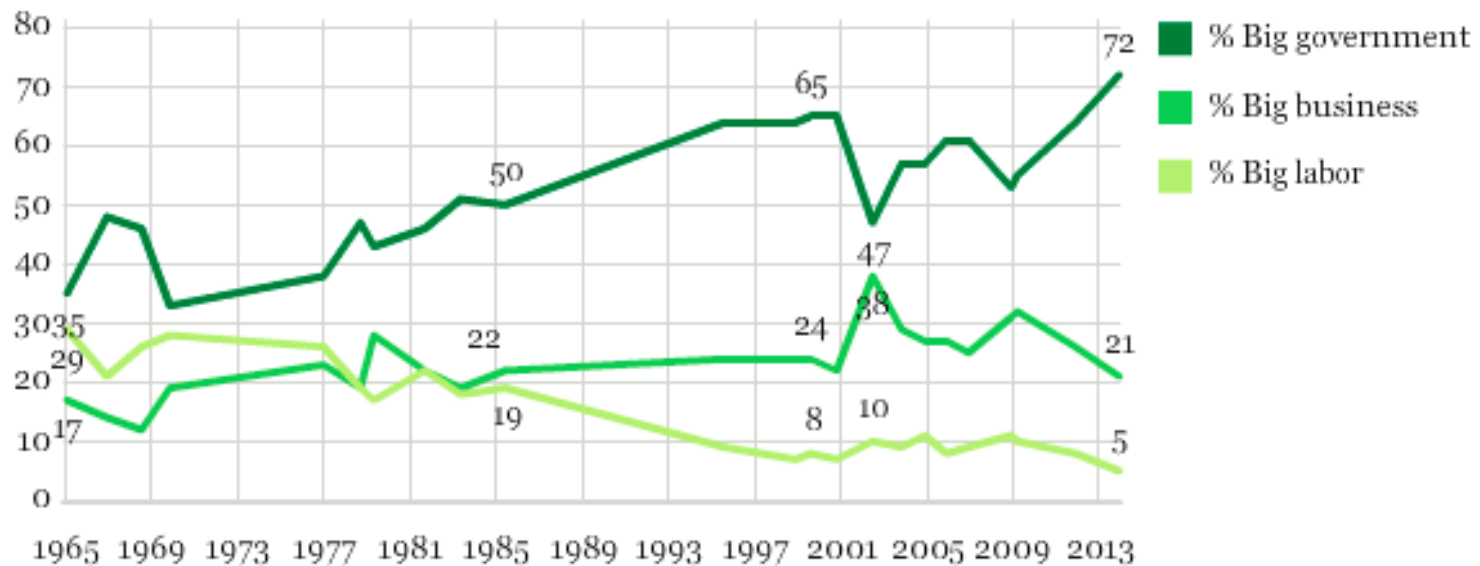
- **Pew Survey:** “... Struggle over privacy and tracking...will extend through the next decade.”
- **Post-Snowden:** 80% say government monitoring is a concern.



# Big government, big worry

## *Views of Biggest Threat to U.S. in Future*

In your opinion, which of the following will be the biggest threat to the country in the future -- big business, big labor, or big government?



GALLUP®

# Activists

- **HackingTeam a Target:**
  - Citizen Lab
  - Human Rights Watch
  - Privacy International
  - Anonymous
  - Threats
- **States Around the World are Targets:**
  - Democracy advocates
  - Human Rights concerns





# Wassenaar Arrangement

- Imposed by E.U.  
Jan. 2015
- Strongest  
regulation on  
exports
- Likely to be  
adopted by the  
U.S.A. this year.

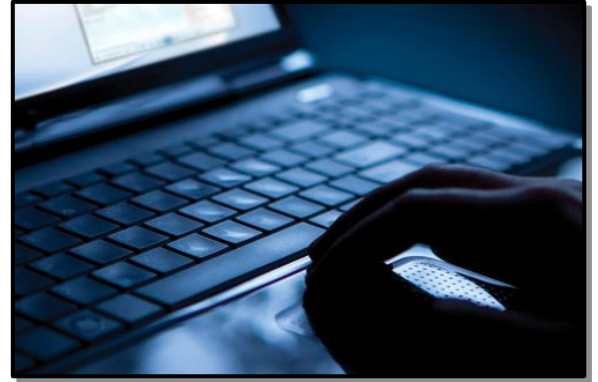


# The Chilling Effect

- Increase regulation...Restrictions on use of technology to fight crime
- Advance of technology slowed or stopped
- Investigators of crime go blind
- Safe refuge for criminals online

# What can Law Enforcement Do?

1. **Speak out** on the need for surveillance
2. Identify for the public the need for a **balance** between **privacy** and **security**
3. **Publicize** successful cases that rely on digital surveillance
4. Pledge to use offensive **surveillance only as allowed by law**
5. **Investigate with care**



# ***Offensive Surveillance:***

***Today's Changing, Challenging and Dangerous  
World and Solutions for Law Enforcement***

Eric Rabe, HackingTeam  
Chief Marketing &  
Communications Officer