Democrazia (digitale) e controllo massivo nell'era post-Datagate

Raoul «Nobody» Chiesa

Founder, President, Security Brokers SCpA

Agenda

- # whoami
- The scenario
- The actors
- Venezuela
- Ukraine
- Privacy and Democracy
- Conclusions
- Books to read
- Stickers! ☺
- Reading Room

Disclaimer

- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers** and **Dr. Web** ones.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

Abstract

- Snowden's leaks **drawn a new border** in the **Intelligence and Cyber Operations world**.

- This presentation will analyze the **concepts of Data Breach** and **Violations of Privacy** after the so-called «Datagate Affair» (NSA scandal), along with the recent happenings in **Kiev** and **Caracas**, then focusing on the concept of **Democracy and Massive Information Control** in the 21th Century.

The Speaker

- President, Founder, **Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Senior Advisor on Cybercrime @ **UNICRI (United Nations Interregional Crime & Justice Research Institute)**
- PSG Member, **ENISA (Permanent Stakeholders Group @ European Union Network & Information Security Agency)**
- Founder, Board of Directors and Technical Commitee Member @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Former Member, Co-coordinator of the WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- **Supporter at various security communities**

We are (were?) used to this….

Everytime we read about a data breach, we do think about the following scenarios and actors.

(Until this guy took a dramatic decision)

Let's stop dreaming!

- In order to «outperform your adversaries», **you must know who they are**.
  - And, over the last 10 years, the concept of «attacker» **has dramatically changed**.

- Also, the **concept** of a «secure systems» doesn't exist anymore. (IMHO).
- Well, actually, it **never existed** ☺
  - Vulnerabilities brought-in by **vendors**
  - **0days** market
  - **State-Sponsored** attacks
  - **DDoS** powershot
  - ……

- Then as I just said, Edward Snowden took **a decision which has changed the whole world**, the **concept of privacy**, **democracy**, and **Intelligence Operations**.

- That's why this presentation **will focus on something different**, trying to walk you by new perspectives, providing **case studies** as well.

The scenario

- Everything «evolved», somehow…
- Here's what United Nations says (Hacker's Profiling Project):

unicri
advancing security, serving justice, building peace

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

And, it’s not just «hackers»

Cybercrime

→ Why «Cybercrime»?

«Cybercrime ranks as one of the top four economic crimes»

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

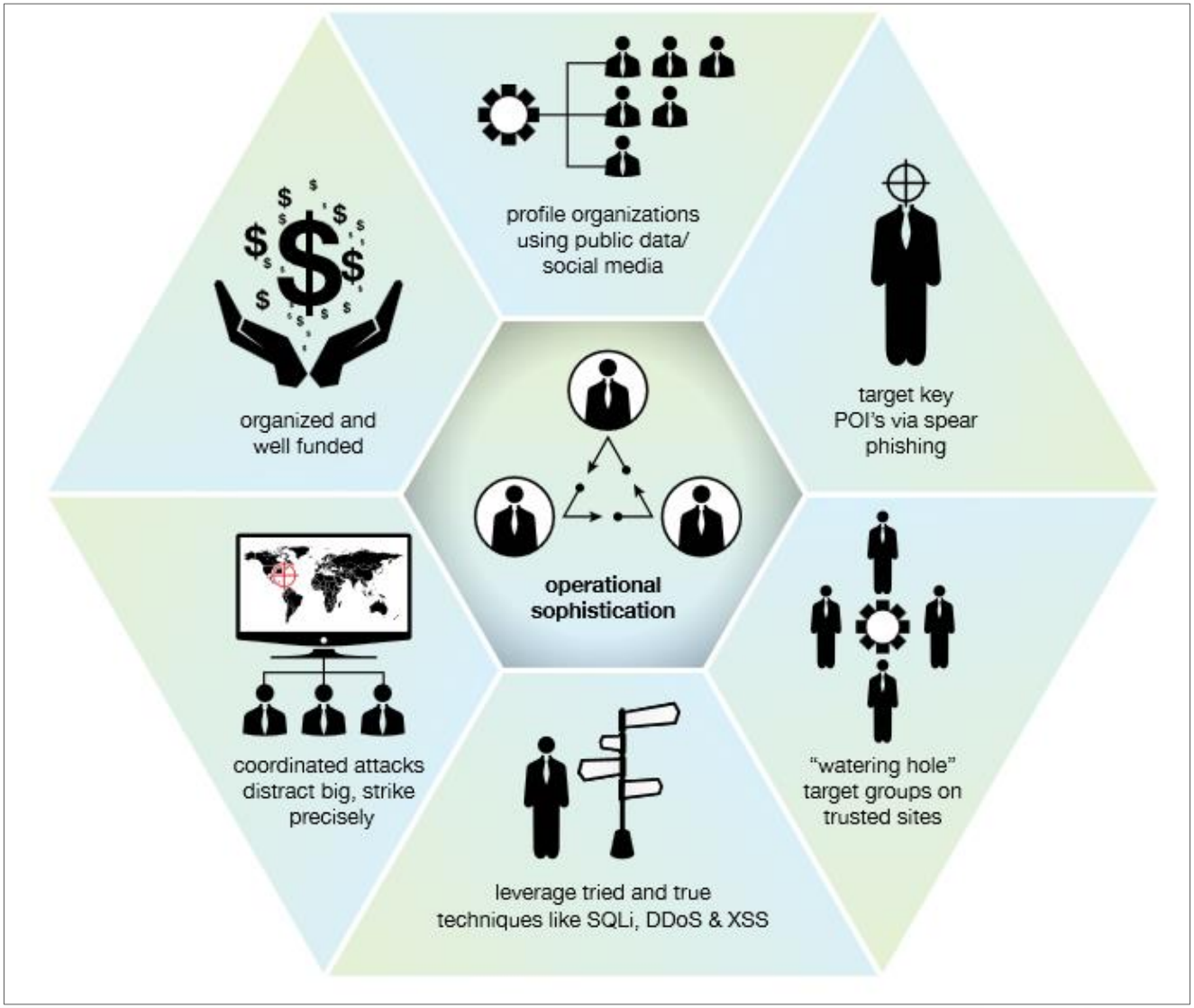
"2011 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

Various sources (UN, USDOJ, INTERPOL, 2011)

Financial Turnover, estimation: 6-12 BLN USD$/year

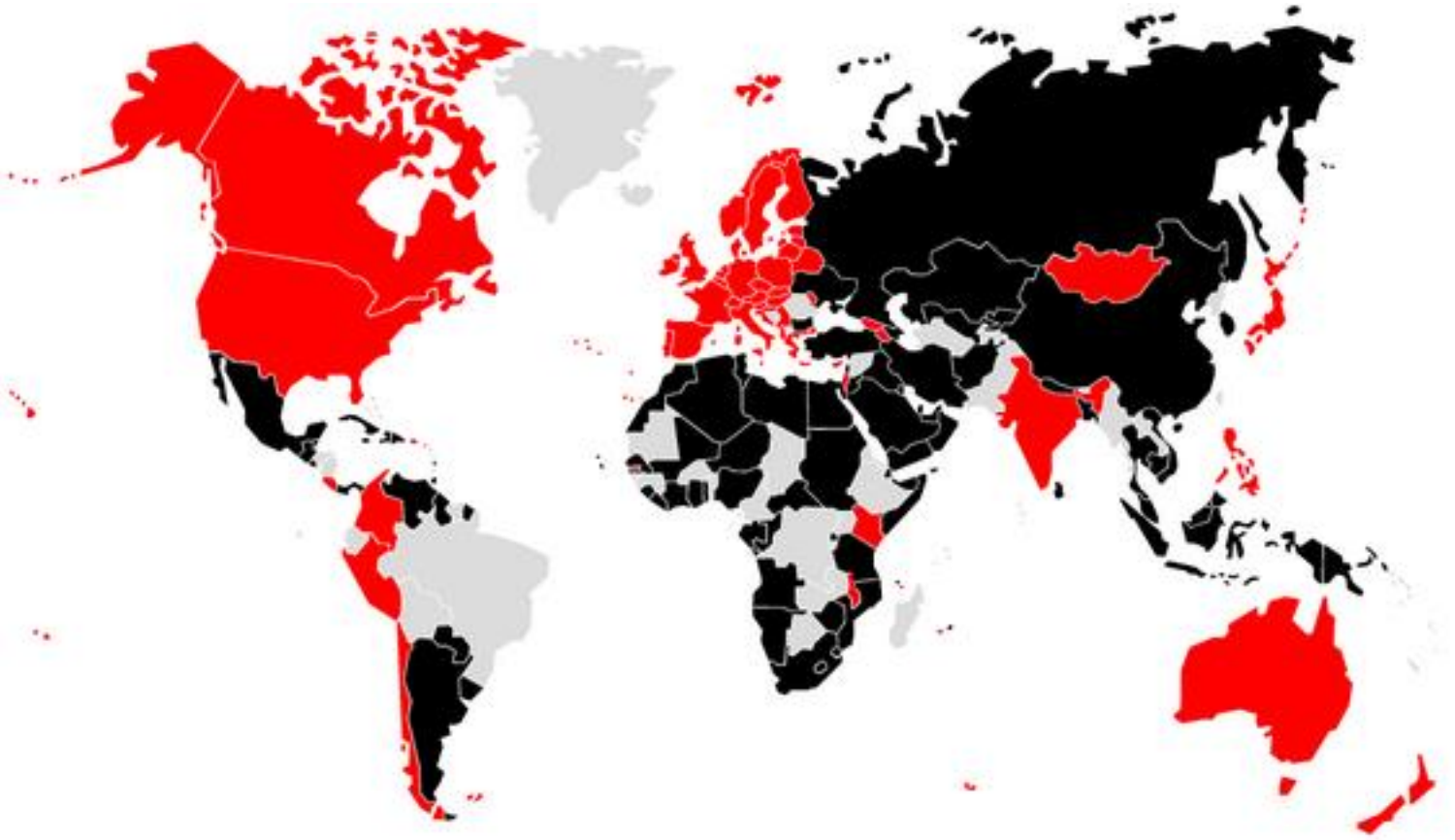
Differences

→ Cybercrime ≠ "hackers"



World

→ Geopolitical shift : 2013 - Map of ITU Dubai General Assembly December (red=not signed; black=signed)



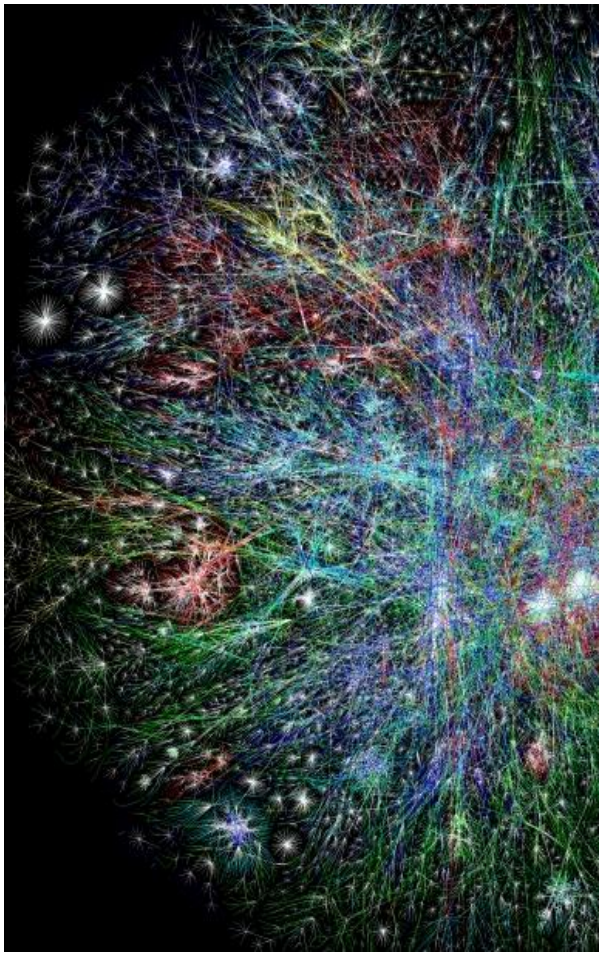
Source: Flavia Zappa,
Security Brokers, 2013

WHAT'S HAPPENING RIGHT NOW

- **Cybercrime and Information Warfare** have a **very wide spectrum of action** and use **intrusion techniques** which are nowadays, somehow, available to a **growing amount of Actors**, which use them in order to **accomplish different goals**, with **approaches and intensity which may deeply vary**.

- **All of the above is launched against any kind of targets:** Critical Infrastructures, Governative Systems, Military Systems, Private Companies of any kind, Banks, Medias, Interest Groups, Private Citizens....
  - **National States**
  - **IC / LEAs**
  - Organized Cybercrime
  - Hacktivists
  - Industrial Spies
  - Terrorists
  - Corporations
  - Cyber Mercenaries

Everyone against everybody

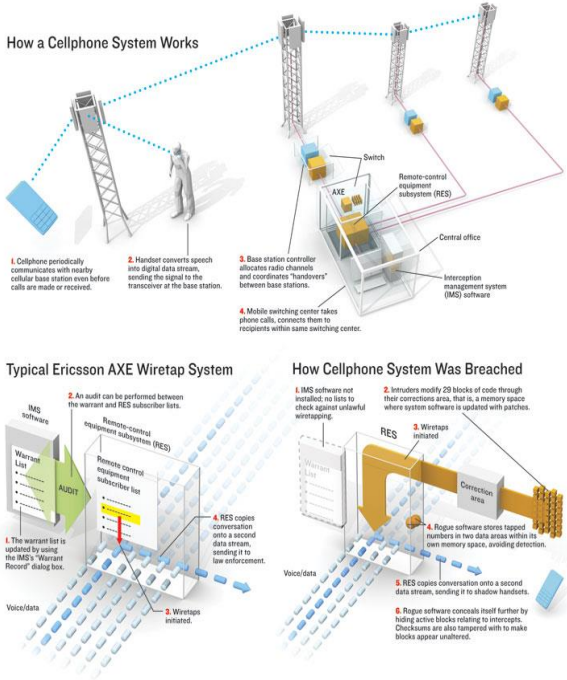


Back in 2005… (?)

→ …«Privacy?!?»

- Vodafone Greece 2004 (“The Athens affair”)
  - ✓ Rootkit on MSC Ericsson AXE
  - ✓ Inbound and Outbound Voice calls, SMS in/out, forwarded to 14 “pay-as-you-go” SIM cards (anonymous ones)
  - ✓ Olympic Games
  - ✓ 14 DEC 2007: Vodafone GR fined with 76M€
  - http://spectrum.ieee.org/telecom/security/the-athens-affair
  - http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005

The illegally wiretapped cellphones in the Athens affair included those of the prime minister, his defense and foreign affairs ministers, top military and law enforcement officials, the Greek EU commissioner, activists, and journalists.

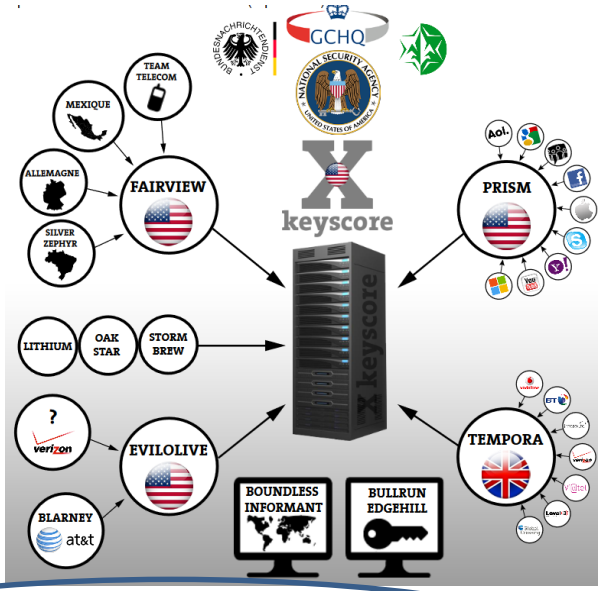


Ahhhhh…. now I get it!

→ …«Privacy?!?»

- ❑ PRISM and other secret project's scandals ("the Snowden case")
- ❑ NSA's budgets for black operations revealed

- http://rt.com/usa/snowden-leak-black-budget-176/
- http://rt.com/usa/us-hacking-exploits-millions-104/
- http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
- http://www.repubblica.it/tecnologia/2013/08/31/news/sall_nsa_231_cyber-attacchi_nel_2011_cos_colpiva_l_intelligence_americana-65600302/



NSA Laughs at PCs, Prefers Hacking Routers and Switches

BY KIM ZETTER 09.04.13 6:30 AM

Follow @KimZetter

Share 1.6k Tweet 1,116 +1 257 Share 231

Home / USA /

The US government might be the biggest hacker in the world

Published time: May 10, 2013 17:08

Edited time: May 12, 2013 15:38

Get short URL

NSA «black-ops Budget» exposed

- NSA's "black budget": 652M$ (2011)
- 231 black operation until today (2011)
- 16 US agencies involved from the US Intelligence community (107.035 employees)

- Targets: US intelligence agencies high priority:
  - ✓ Iran
  - ✓ Russia
  - ✓ China
  - ✓ Afghanistan
  - ✓ North Korea
  - ✓ Syria
  - ✓ ……

The Washington Post

- Cyber Attacks Unit "GENIE"
- Hacking into foreign systems in order to spy on contents, controlling functions
- http://articles.washingtonpost.com/2013-08-29/world/41709796_1_intelligence-community-intelligence-spending-national-intelligence-program

What happened on September 2013?

Belgian Telco says it was hacked, while reports point to NSA or GCHQ as culprit

http://gigaom.com/2013/09/16/belgian-telco-says-it-was-hacked-while-reports-point-to-nsa-or-gchq-as-culprit/

And the Police is asking for more powers

Home > Security > Cybercrime and Hacking

News

Dutch bill would give police hacking powers

Dutch law enforcement should be allowed to break into computers outside the Netherlands when necessary, the draft bill said

By Loek Essers

May 2, 2013 06:47 AM ET Add a comment

Share 8+1 Like 0 More

IDG News Service - The Dutch government today presented a draft bill that aims to give law enforcement the power to hack into computer systems -- including those located in foreign countires -- to do research, gather and copy evidence or block access to certain data.

Law enforcement should be allowed to block access to child pornography, read emails that contain information exchanged between criminals and also be able to place taps on communication, according to a draft bill published Thursday and signed by Ivo Opstelten, the Minister of Security and Justice. Government agents should also be able to engage in activities such as turning on a suspect's phone GPS to track their location, the bill said.

Opstelten announced last October he was planning to craft this bill.

Dutch Government Seeks to Let Law Enforcement Hack Foreign Computers

Dutch government wants to give law enforcement agencies investigative powers that involve hacking, installing spyware and destroying data

By Lucian Constantin
Fri, October 19, 2012

1 Comment

IDG News Service — The Dutch government wants to give law enforcement authorities the power to hack into computers, including those located in other countries, for the purpose of discovering and gathering evidence during cybercrime investigations.

In a letter that was sent to the lower house of the Dutch parliament on Monday, the Dutch Minister of Security and Justice Ivo Opstelten outlined the government's plan to draft a bill in upcoming months that would provide law enforcement authorities with new investigative powers on the Internet.

According to the letter, the new legislation would allow cybercrime investigators to remotely infiltrate computers in order to install monitoring software or to search them for evidence. Investigators would also be allowed to destroy illegal content, like child pornography, found during such searches.

These investigative powers would not only cover computers located in the Netherlands, but also computers located in other countries, if the location of those computers cannot be determined.


NOVEMBER 28, 1983
$1.75
TIME
NUCLEAR ARMS
Troubled Talks And Angry Protests
1984
Big Brother's Father
Author
George Orwell


TIME
PERSON OF THE YEAR

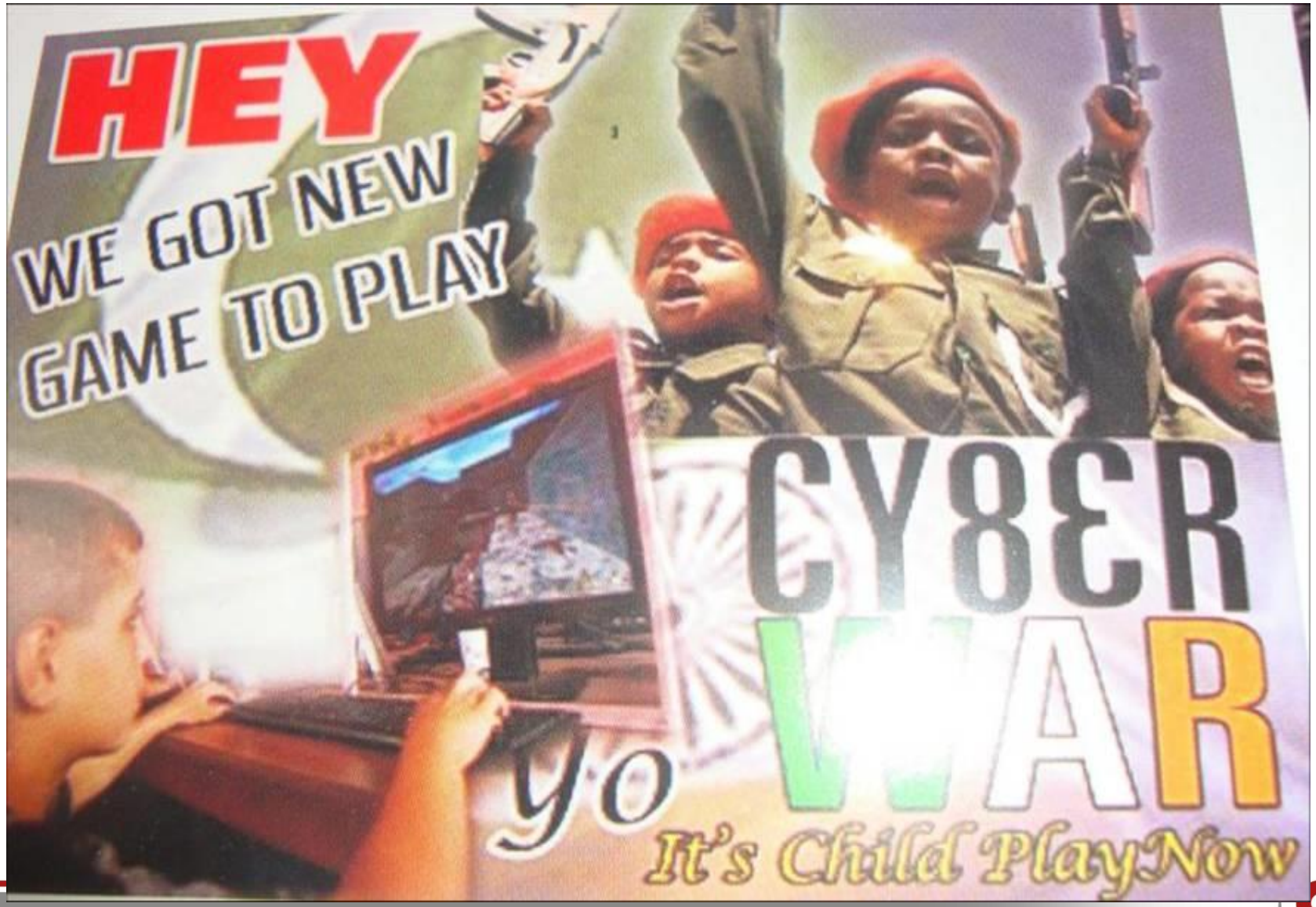
Hmmmmmm…….


Den Norske Nobelkomite
har overensstemmende med
reglene i det av
ALFRED NOBEL
den 27 november 1895
opprettede testamente tildelt
Barack H. Obama
Nobels Fredspris
for 2009

Maybe…… ☺


TIME
PERSON OF THE YEAR

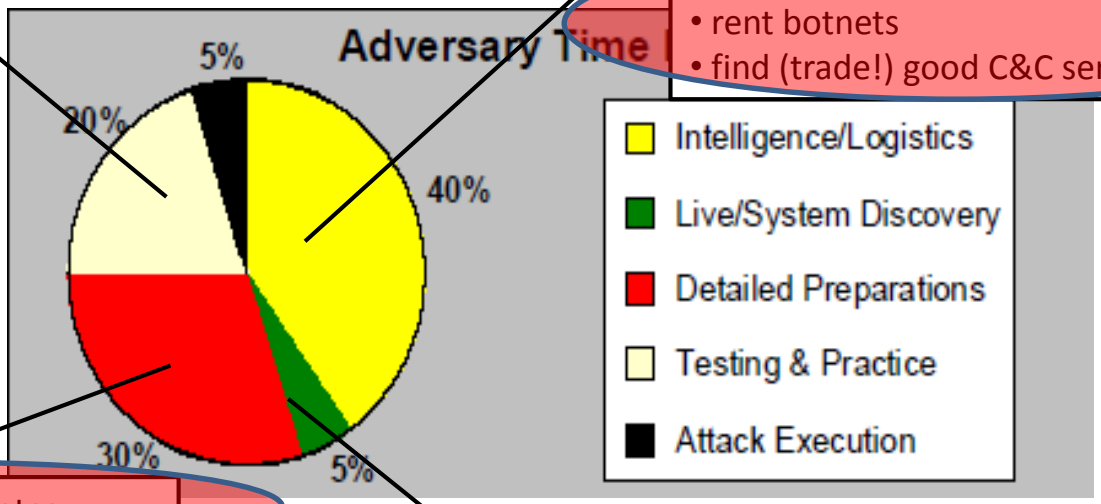

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


HEY
WE GOT NEW
GAME TO PLAY
CY8ER
yo WAR
It's Child PlayNow

Making “Cyber War”…

- equipment to mimic target network
- dummy run on similar network
- sandbox zerodays

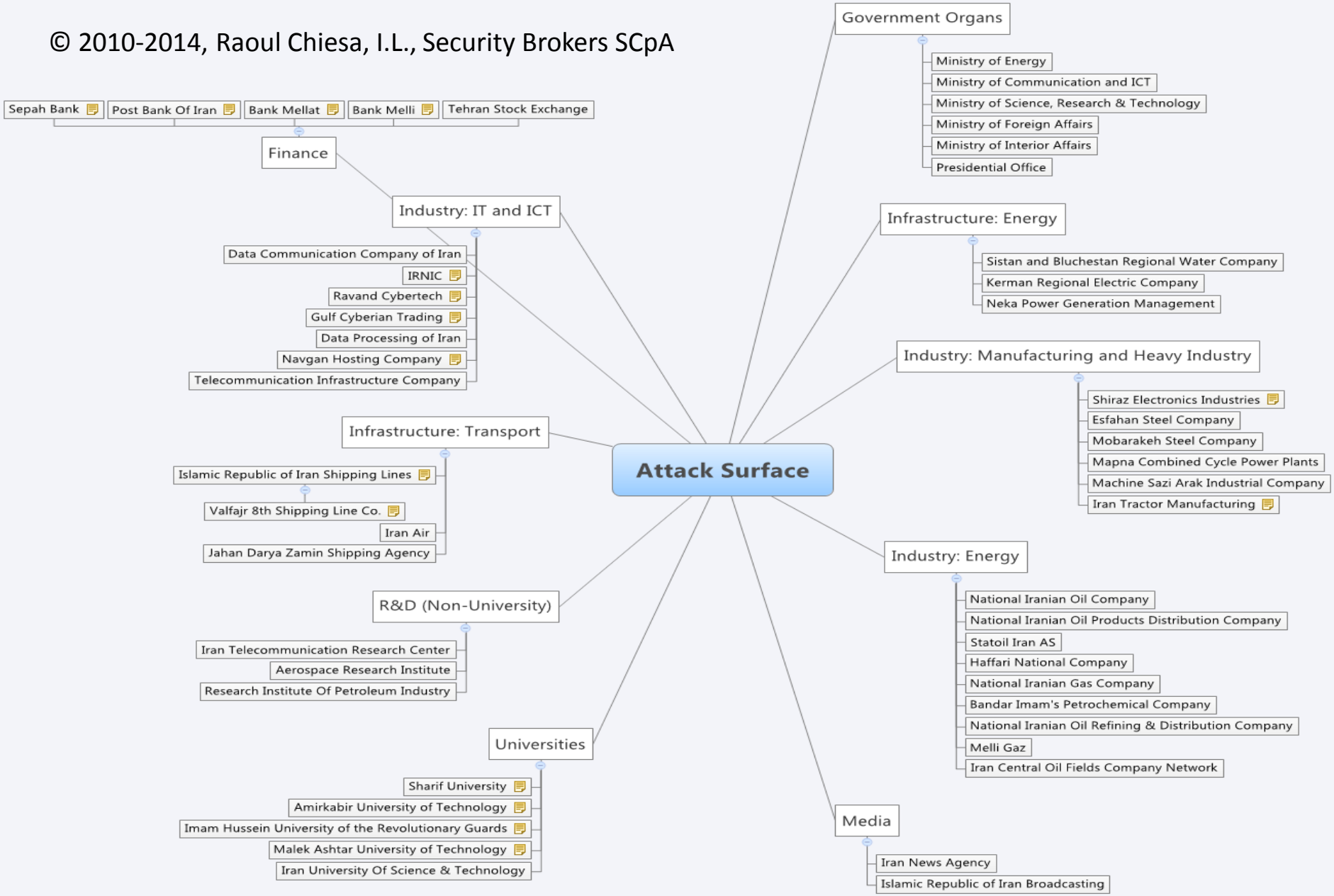
- „dummy list“ of „ID-10T“ for phishing
- background info on organisation (orgchart etc.)
- Primer for sector-specific social-engineering
- proxy servers
- banking arrangements
- purchase attack-kits
- rent botnets
- find (trade!) good C&C server



- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

•Purchase L2/L3 system data

Alexander Klimburg 2012



Scenarios

- OK, you're smart, you've found the **most ever l33t 0day of your life**.

- **Who could buy/trade/whatever** that stuff from you?
  - Some **hacker folks**.
    - (which, eventually, may resell it to one of the following)
  - IT Vendors
  - Security **Vendors**
  - Big **Internet players**
  - 0days «**brokers**»
  - Law Enforcement Agencies (**LEAs**)
  - Intelligence Agencies (**IAs**)
  - Lawful Interception (**LI**) private companies
  - **Cybercrime** / Organized Crime (drugs cartels in Mexico, ever heard about?)
  - **Pwoning contests**, CTFs, etc.
  - (**Hacktivists**?)

https://www.wikileaks.org/the-spyfiles.html

Selling Surveillance to Dictators

When citizens overthrew the dictatorships in Egypt and Libya this year, they uncovered listening rooms where devices from Gamma corporation of the UK, Amesys of France, VASTech of South Africa and ZTE Corp of China monitored their every move online and on the phone.

Surveillance companies like SS8 in the U.S., Hacking Team in Italy and Vupen in France manufacture viruses (Trojans) that hijack individual computers and phones (including iPhones, Blackberries and Androids), take over the device, record its every use, movement, and even the sights and sounds of the room it is in. Other companies like Phoenexia in the Czech Republic collaborate with the military to create speech analysis tools. They identify individuals by gender, age and stress levels and track them based on 'voiceprints'. Blue Coat in the U.S. and Ipoque in Germany sell tools to governments in countries like China and Iran to prevent dissidents from organizing online.

Trovicor, previously a subsidiary of Nokia Siemens Networks, supplied the Bahraini government with interception technologies that tracked human rights activist Abdul Ghani Al Khanjar. He was shown details of personal mobile phone conversations from before he was interrogated and beaten in the winter of 2010-2011.

How Mass Surveillance Contractors Share Your Data with the State

In January 2011, the National Security Agency broke ground on a $1.5 billion facility in the Utah desert that is designed to store terabytes of domestic and foreign intelligence data forever and process it for years to come.

Telecommunication companies are forthcoming when it comes to disclosing client information to the authorities - no matter the country. Headlines during August's unrest in the UK exposed how Research in Motion (RIM), makers of the Blackberry, offered to help the government identify their clients. RIM has been in similar negotiations to share BlackBerry Messenger data with the governments of India, Lebanon, Saudi Arabia, and the United Arab Emirates.

Weaponizing Data Kills Innocent People

There are commercial firms that now sell special software that analyze this data and turn it into powerful tools that can be used by military and intelligence agencies.

HACKING TEAM RCS

Suspected Government Users Worldwide

Citizen Lab 2014

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

21 SUSPECTED GOVERNMENT USERS

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

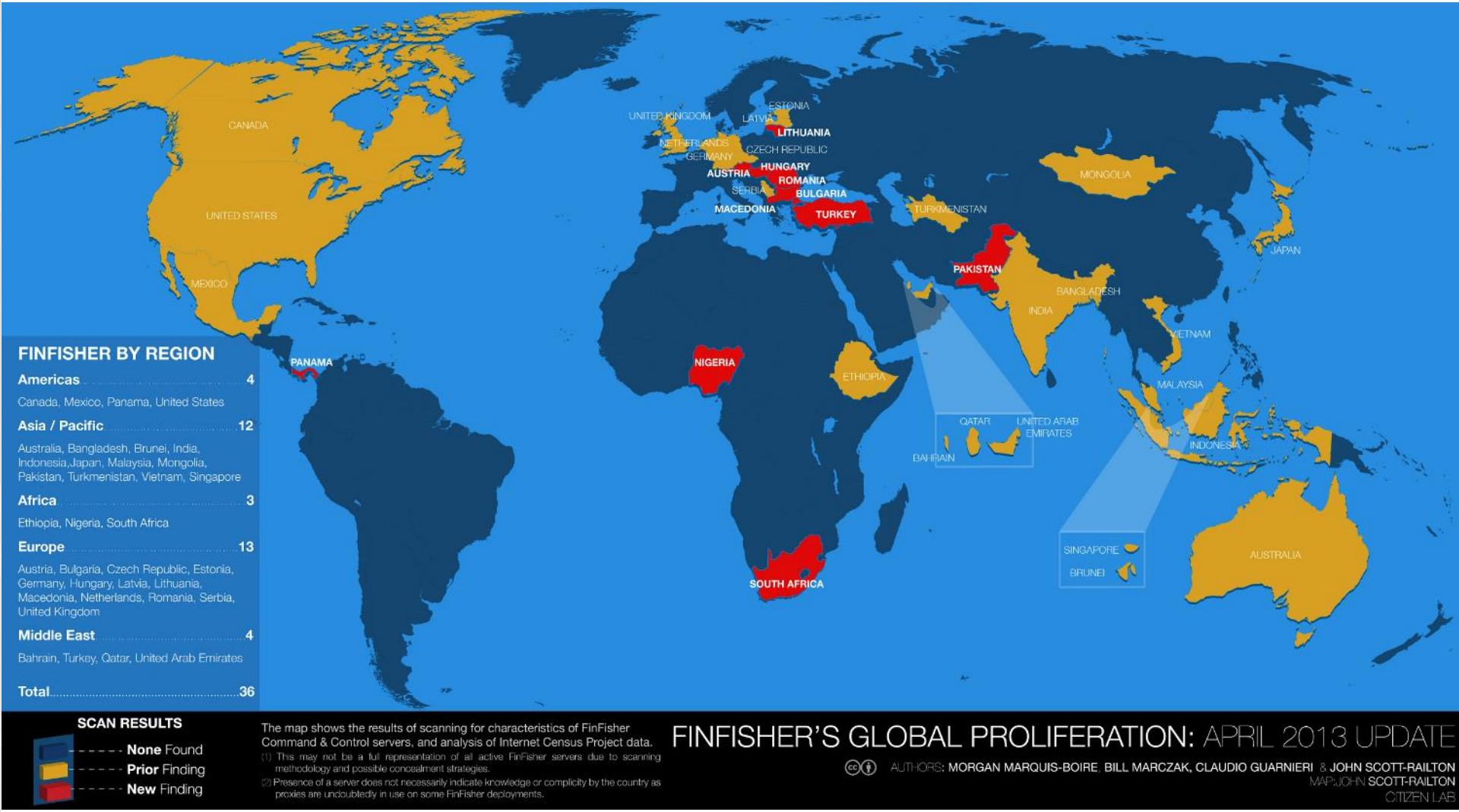
CAUSE FOR CONCERN

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

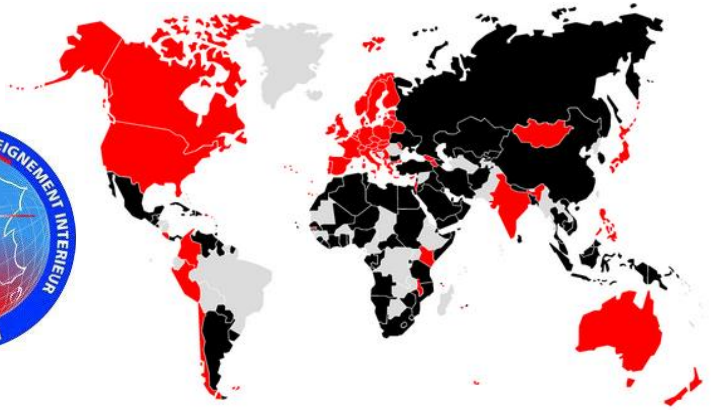
Finfisher


CANADA
UNITED STATES
MEXICO
PANAMA
UNITED KINGDOM
ESTONIA
LATVIA
LITHUANIA
NETHERLANDS
GERMANY
CZECH REPUBLIC
AUSTRIA
HUNGARY
ROMANIA
SERBIA
BULGARIA
MACEDONIA
TURKEY
NIGERIA
ETHIOPIA
SOUTH AFRICA
TURKMENISTAN
MONGOLIA
PAKISTAN
BANGLADESH
INDIA
JAPAN
VIETNAM
MALAYSIA
QATAR
UNITED ARAB EMIRATES
BAHRAIN
INDONESIA
SINGAPORE
BRUNEI
AUSTRALIA
FINFISHER BY REGION
Americas 4
Canada, Mexico, Panama, United States
Asia / Pacific 12
Australia, Bangladesh, Brunei, India, Indonesia, Japan, Malaysia, Mongolia, Pakistan, Turkmenistan, Vietnam, Singapore
Africa 3
Ethiopia, Nigeria, South Africa
Europe 13
Austria, Bulgaria, Czech Republic, Estonia, Germany, Hungary, Latvia, Lithuania, Macedonia, Netherlands, Romania, Serbia, United Kingdom
Middle East 4
Bahrain, Turkey, Qatar, United Arab Emirates
Total 36
SCAN RESULTS
None Found
Prior Finding
New Finding
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

Global, dirty business

- "Mass interception of entire populations is not only a reality, it is a secret new industry spanning **25 countries**."
- "It's estimated that the global computer surveillance technology market is worth **$5 billion a year**."
  - ITALY: **300M/year**

Who do you wanna sell (your 0days) to?



Bundesamt
für Sicherheit in der
Informationstechnik

IMMUNITY

SIEMENS

]HackingTeam[

paloalto NETWORKS

VUPEN security

The pricing debate

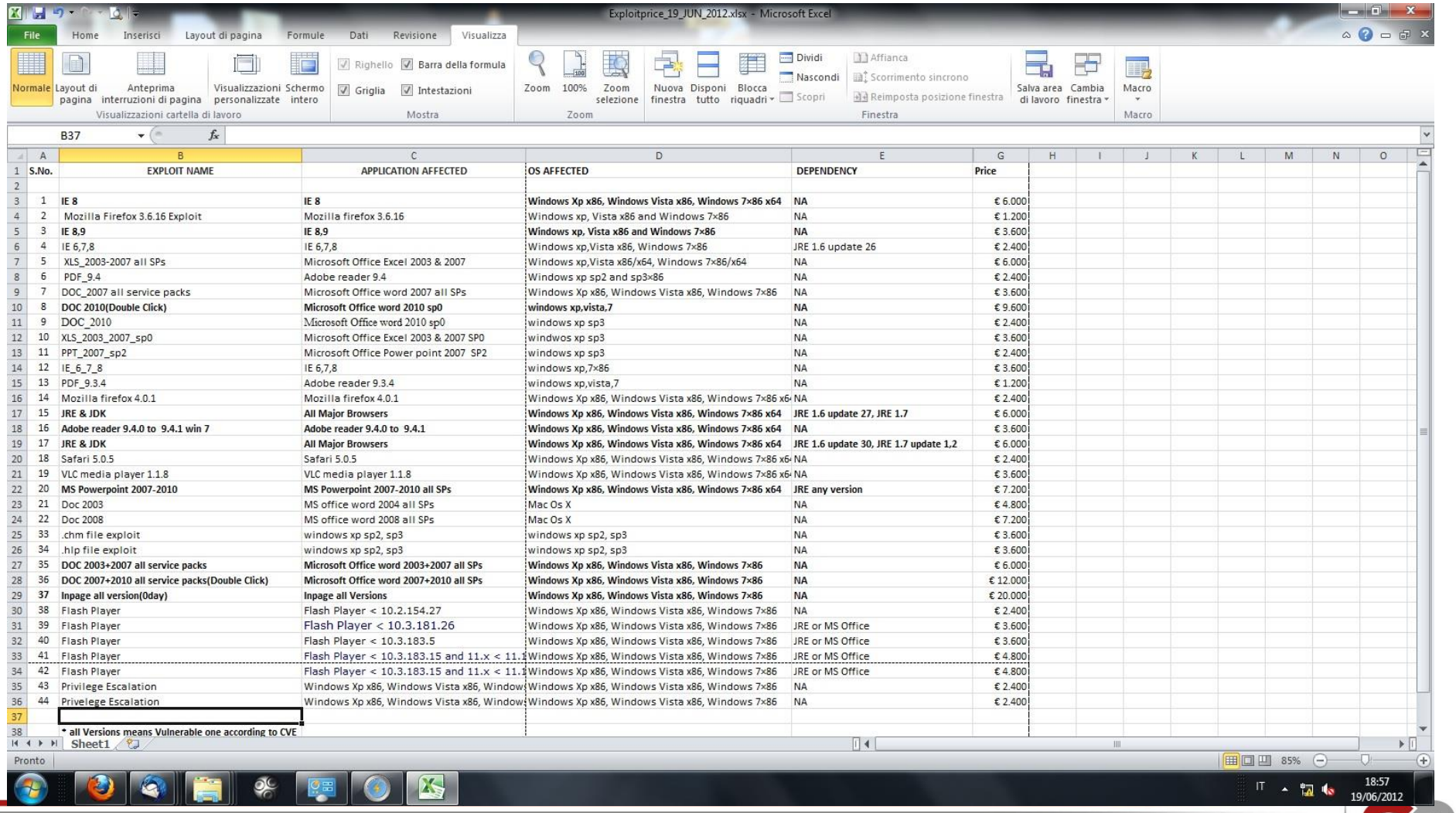
- I think all of you remember this:

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Source: Forbes, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", 2012, in http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

The pricing debate

- What about this? (CHEAP but LAME, India's ones)



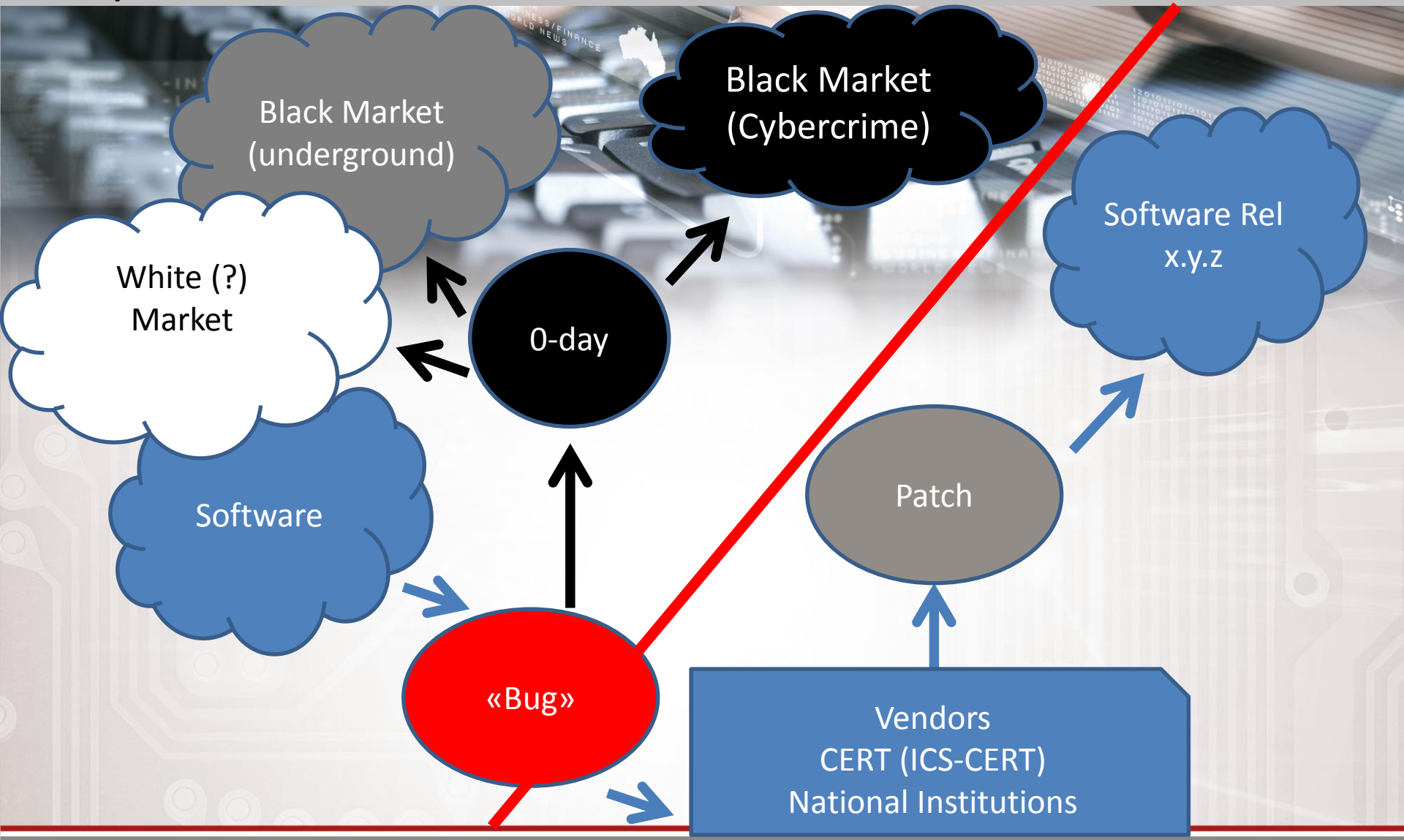
S.No.	EXPLOIT NAME	APPLICATION AFFECTED	OS AFFECTED	DEPENDENCY	Price
1	**IE 8**	**IE 8**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**NA**	€ 6.000
2	Mozilla Firefox 3.6.16 Exploit	Mozilla firefox 3.6.16	Windows xp, Vista x86 and Windows 7×86	NA	€ 1.200
3	**IE 8,9**	**IE 8,9**	**Windows xp, Vista x86 and Windows 7×86**	**NA**	€ 3.600
4	IE 6,7,8	IE 6,7,8	Windows xp,Vista x86, Windows 7×86	JRE 1.6 update 26	€ 2.400
5	XLS_2003-2007 all SPs	Microsoft Office Excel 2003 & 2007	Windows xp,Vista x86/x64, Windows 7×86/x64	NA	€ 6.000
6	PDF_9.4	Adobe reader 9.4	Windows xp sp2 and sp3×86	NA	€ 2.400
7	DOC_2007 all service packs	Microsoft Office word 2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 3.600
8	**DOC 2010(Double Click)**	**Microsoft Office word 2010 sp0**	**windows xp,vista,7**	**NA**	€ 9.600
9	DOC_2010	Microsoft Office word 2010 sp0	windows xp sp3	NA	€ 2.400
10	XLS_2003_2007_sp0	Microsoft Office Excel 2003 & 2007 SP0	windwos xp sp3	NA	€ 3.600
11	PPT_2007_sp2	Microsoft Office Power point 2007 SP2	windows xp sp3	NA	€ 2.400
12	IE_6_7_8	IE 6,7,8	windows xp,7×86	NA	€ 3.600
13	PDF_9.3.4	Adobe reader 9.3.4	windows xp,vista,7	NA	€ 1.200
14	Mozilla firefox 4.0.1	Mozilla firefox 4.0.1	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 2.400
15	**JRE & JDK**	**All Major Browsers**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE 1.6 update 27, JRE 1.7**	€ 6.000
16	**Adobe reader 9.4.0 to 9.4.1 win 7**	**Adobe reader 9.4.0 to 9.4.1**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**NA**	€ 3.600
17	**JRE & JDK**	**All Major Browsers**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE 1.6 update 30, JRE 1.7 update 1,2**	€ 6.000
18	Safari 5.0.5	Safari 5.0.5	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 2.400
19	VLC media player 1.1.8	VLC media player 1.1.8	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 3.600
20	**MS Powerpoint 2007-2010**	**MS Powerpoint 2007-2010 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE any version**	€ 7.200
21	Doc 2003	MS office word 2004 all SPs	Mac Os X	NA	€ 4.800
22	Doc 2008	MS office word 2008 all SPs	Mac Os X	NA	€ 7.200
33	.chm file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
34	.hlp file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
35	**DOC 2003+2007 all service packs**	**Microsoft Office word 2003+2007 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 6.000
36	**DOC 2007+2010 all service packs(Double Click)**	**Microsoft Office word 2007+2010 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 12.000
37	**Inpage all version(0day)**	**Inpage all Versions**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 20.000
38	Flash Player	Flash Player < 10.2.154.27	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400
39	Flash Player	Flash Player < 10.3.181.26	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 3.600
40	Flash Player	Flash Player < 10.3.183.5	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 3.600
41	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 4.800
42	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 4.800
43	Privilege Escalation	Windows Xp x86, Windows Vista x86, Window	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400
44	Privilege Escalation	Windows Xp x86, Windows Vista x86, Window	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400

* all Versions means Vulnerable one according to CVE

Where’s the truth?

What’s the right approach with pricing?

→ 0-day Markets



A different (more serious?) approach

Public Knowledge of the vulnerability	Buyer's typology IS = IT Security companies INT = Intelligence Agencies for Governmental use (National Security protection) MIL = MoD/related actors for warfare use OC = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	IS	10K – 50K USD
Y	INT	30K – 150K USD
Y	MIL	50K – 200K USD
Y	OC	5K – 80K USD
N	ALL	X2 – X10

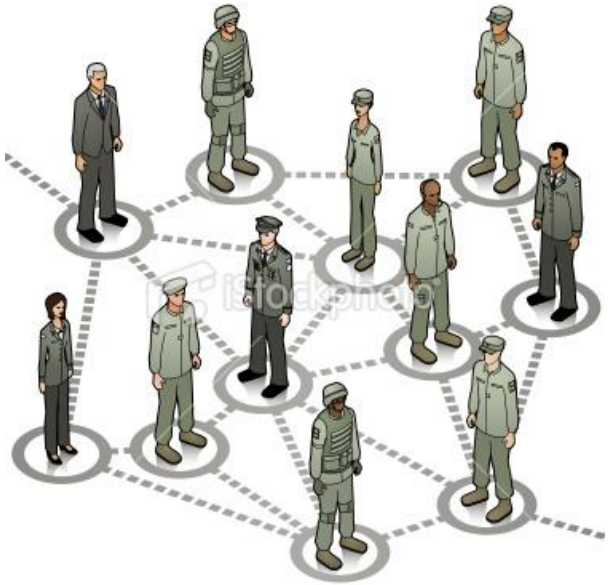
A different (more serious?) approach

Public Knowledge of the vulnerability	Vulnerability relays on: Operating System (OS) Major General Applications (MGA) SCADA-Industrial Automation (SCADA)	Buyer's typology IS = IT Security companies INT = Intelligence Agencies for Governmental use (National Security protection) MIL = MoD/related actors for warfare use OC = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	OS	OC	40K – 100K
Y	MGA	INT	100K – 300K
Y	SCADA	MIL	100K – 300K
N	OS	MIL	300K – 600K
N	SCADA	MIL	400K – 1M

So, guys….

→ «Privacy?!?»

The DUMA…. knew!!



"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers

This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.

Former Duma speaker Nikolai Kuryanovich, 2007

Hackers as a National Resource?

- In the last year I've dig into a research from an **Hungarian security researcher** from **HP**
- His **idea** was **weird**!

- Should we **consider hackers** as "the enemy" / "troubles"…
- …Or, may they represent an **opportunity for Governments**??
  - ✓ **Patriot's** Hackers
  - ✓ Think about **bloggers** and **North Africa / GCC Area** (Gulf Countries)
  - ✓ Think about **IRAN** and **Twitter**
  - ✓ See the **potentialities**?


Feds Seek a Few Good Hacke
www.pcworld.com/article/117226/feds_seek_a_few_good_hackers.html
Other Bookmarks
Most Visited
Socials
Tools
Search
Sign in | Join Us | Newsletters |
PCWorld
News
Reviews
How-To's
Downloads
Shop & Compare
Apps
Business Center
holiday Gift guide
Magazine
Subscribe & Get a Bonus CD
Customer Service
I.T.
ENGLISH
KEEPS BAD STUFF OFF YOUR PC.
webroot
Personal Security
PERFECT PRINT SOLUTIONS
Find just the right All-in-One Printer for you from HP.
Visit the Print Solutions Center.
PRINT WITHOUT A PC
See the world's first Web-connected home printer with web apps.
Visit the Printing Solutions Center
PCWorld » Security
Like
Tweet
0
0
Digg
0 Comments
+ recommends
Email
Print
RSS
Feds Seek a Few Good Hackers
War on terrorism distracts cybercops from routine hacking, and even encourages alliances.
By Andrew Brandt, PCWorld Aug 4, 2004 4:00 am
Attention, hackers: Uncle Sam wants you.
And hackers are answering the call, or at least listening. A well-attended session at the recent Defcon 12 hackers' conference was "Meet the Feds," a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would-be cybercops.
"We're looking for good, talented people. We need a lot of help," said Jim Christy, director of the Defense Department's Cyber Crime Center.
"The Department of Defense understands how important computers are to defending the United States, and is always on the lookout for good people," said Alvin Wallace, a supervisory special agent with the Air Force's Office of Special Investigations.
Patriotic Hackers Sought
pctools

Hacker 'Mudge' gets DARPA

news.cnet.com/8301-27080_3-10450552-245.html

Other Bookmarks

Most Visited | Socials | Tools

log in | join CNET

home | reviews | news | downloads | video | On CHOW: An iPhone app for Thanksgiving!

cnet news

Latest News | CNET River BETA | Webware | Crave | Business Tech | Green Tech | Wireless | Security | Blogs | More

February 10, 2010 4:00 AM PST

Hacker 'Mudge' gets DARPA job

Font size | Print | E-mail | Share | 14 comments

by Elinor Mills

Tweet 1 | Share 175

Peiter Zatko--a respected hacker known as "Mudge"--has been tapped to be a program manager at DARPA, where he will be in charge of funding research designed to help give the U.S. government tools needed to protect against cyberattacks, CNET has learned.

Zatko will become a program manager in mid-March within the Strategic Technologies Office at **DARPA** (Defense Advanced Research Projects Agency), which is the research and development office for the Department of Defense. His focus will be cybersecurity, he said in an interview with CNET on Tuesday.

One of his main goals will be to fund researchers at hacker spaces, start-ups, and boutiques who are most likely to develop technologies that can leapfrog what comes out of large corporations. "I want revolutionary changes. I don't want evolutionary ones," he said.

He's also hoping that giving a big push to research and development will do more to advance the progress of cybersecurity than public policy decisions have been able to

Most Popular

- IE9 the best browser? Not so fast
- Jammie Thomas hit with $1.5 million verdict
- Facebook to Foursquare: You're out
- Get a 1TB external hard drive for $47.59
- Kinect's launch day bumps and triumphs

CNET River | log in | join CNET

My Lists | TechTracker

Voltiamo pagina

Caracas: «No Internet, please!»

Una lista dei servizi internet bloccati in Venezuela

Twitter, Zello e Pastebin sono stati resi inutilizzabili in parte o del tutto e il governo ha ritirato i tesserini alla CNN.

Questo articolo è apparso originariamente su IBTimes.com

Con la protesta che monta e l'attenzione internazionale sempre più concentrata sul Venezuela, il governo del Presidente Maduro ha intensificato l'opera di censura dei media bloccando diversi siti e strumenti di aggregazione per gli attivisti.

È complicato accertare quali portali siano realmente stati oscurati, il che fa pensare che i blocchi non siano poi così efficaci. Sotto c'è una lista di siti, app e servizi che sono risultati inutilizzabili nei giorni scorsi (alcuni lo sono ancora adesso) in Venezuela.

Twitter – Il governo ha bloccato la funzione che permette di caricare immagini dopo che la scorsa settimana le foto della polizia impegnata a reprimere la protesta avevano invaso la rete. Ora il servizio è stato

Caracas: (no comment)

Caracas: hacktivism

Caracas: hacktivism

ЄВРОМАЙДАН @euromaidan · 4 h
Fight for your freedom. #OpVenezuela #lasalida #Venezuela #PrayForVenezuela #SOSVenezuela #F12 #F13 #F14 pic.twitter.com/w4sH1TMm4C

Risposta Retweet Preferito Segnala contenuto

blogs.wsj.com/cio/2014/03/04/the-morning-download-ukraine-claims-telecom-system-hacked/

CIO Journal.

CIO Report | Consumerization | Big Data | Cloud | Talent & Management | Security

March 4, 2014, 8:30 AM ET

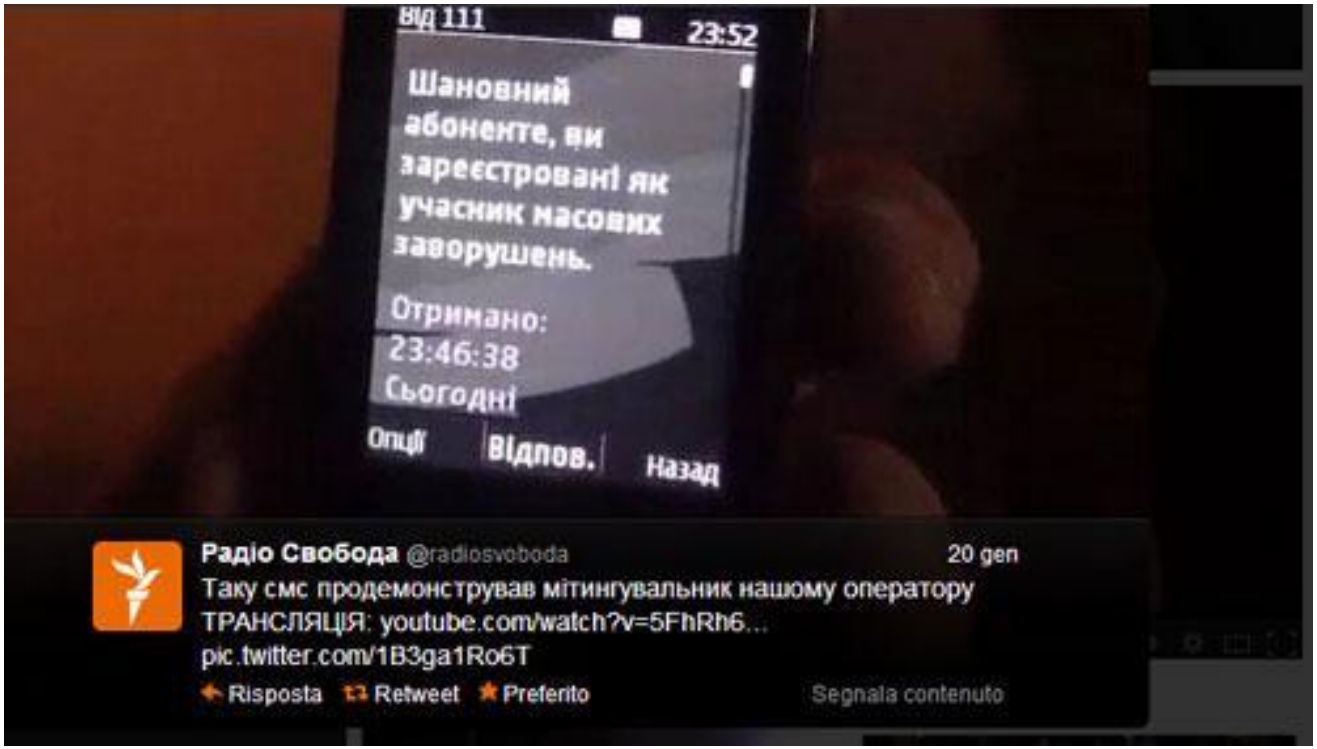
The Morning Download: Ukraine Claims Telecom System Hacked

Article | Comments

By MICHAEL HICKINS CONNECT

Editor

(ab)using Geolocalization



http://www.ilfattoquotidiano.it/2014/01/23/ucraina-il-grande-fratello-controlla-la-piazza-via-sms/855088/

(ab)using Geolocalization

www.ilfattoquotidiano.it/2014/01/23/ucraina-il-grande-fratello-controlla-la-piazza-via-sms/855088/

Sei in: Il Fatto Quotidiano > Blog di Umberto Rapetto > Ucraina, il Gra...

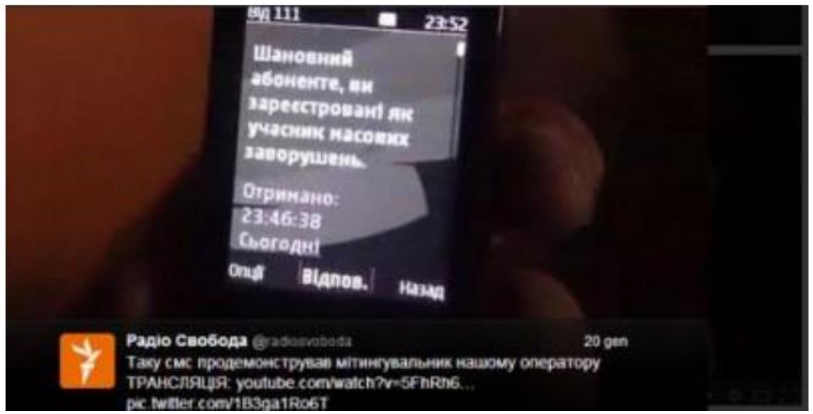
Ucraina, il Grande Fratello controlla la piazza via sms?

di Umberto Rapetto | 23 gennaio 2014 Commenti (85)

Più informazioni su: George Orwell, Kiev, Manifestazioni, SMS, Ucraina, Unione Europea.

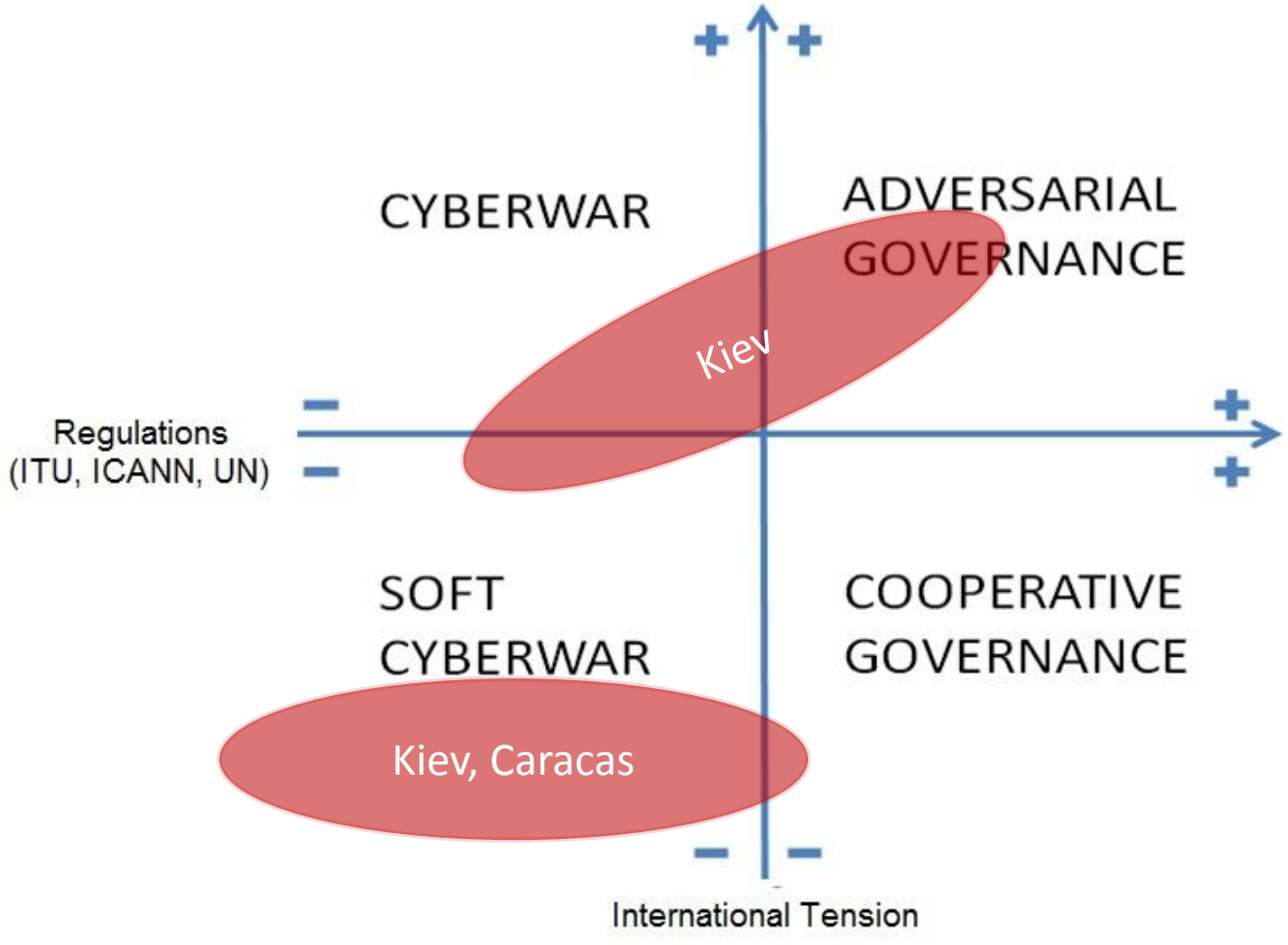
8

g+1



"Carissimo abbonato, abbiamo registrato il suo nominativo come partecipante ad una manifestazione di disturbo di massa": è questo il testo di un sms che sarebbe giunto sui telefonini dei dimostranti in un evento di protesta tenutosi nella giornata di martedì 21 gennaio a Kiev.

Evolving scenarios: 2014-2017



So what….?

- **Scenarios and happenings which were not «mandatory» including massive information control on the citiziens, are now a reality.**

- ***Governments are abusing of the technologies.***
  - ***With the support of private companies.***
  - ***Acting just like the Organized Crime and the Cybercrime is doing.***

- ***We MUST do something. Now!***

- ***The reason is VERY EASY***

(see next 4 slides)

TED
Ideas worth spreading

http://video.ted.com/talk/podcast/2013X/None/MikkoHypponen_2013X-480p.mp4

Quoting Mikko /1

«Gli americani sono pronti a **buttare via la Costituzione**, buttarla nel cestino, solo **perché ci sono i terroristi?** La stessa cosa per il ***Bill of Rights*** (la Carta del Diritti) e tutti gli emendamenti, la **Dichiarazione Universale dei Diritti dell'Uomo**, le **convenzioni europee sui diritti dell'uomo** e le **libertà fondamentali** e la **libertà di stampa**? **Pensiamo veramente che il terrorismo sia una tale minaccia esistenziale da essere disposti a fare qualunque cosa?»**

Quoting Mikko /2

«La **sorveglianza cambia la storia**. Lo sappiamo da esempi di **presidenti corrotti come Nixon**. Immaginate se avesse avuto il **tipo di strumenti di sorveglianza** disponibili oggi. Fatemi **citare testualmente** il presidente del Brasile, la signora **Dilma Rousseff**. È stata uno degli **obiettivi della sorveglianza della NSA**. Le sue **mail sono state lette**, e lei ha parlato alla **sede delle Nazioni Unite** e ha detto»:

Hello Miss President…. ☹

(Discorso alle Nazioni Unite a New York)

*«Se non c'è nessun diritto alla **privacy**,*
*non può esistere nessuna **vera libertà di espressione e opinione**, e quindi non può esistere*
*una **democrazia efficace**.»*

- Ecco di cosa si tratta.
- La privacy è il mattone fondamentale delle nostre democrazie.
- E per citare un collega ricercatore della sicurezza, Marcus Ranum, «gli Stati Uniti oggi stanno **trattando Internet come se fosse una delle loro colonie**.»
  - «Siamo tornati all'epoca della colonizzazione, e noi, gli "stranieri" che usiamo Internet, dovremmo vedere gli Americani come i nostri padroni.»

Datagate e CyberWar

Il problema principale che vedo è l'**awareness**, l'**informazione**, la **sensibilizzazione**.

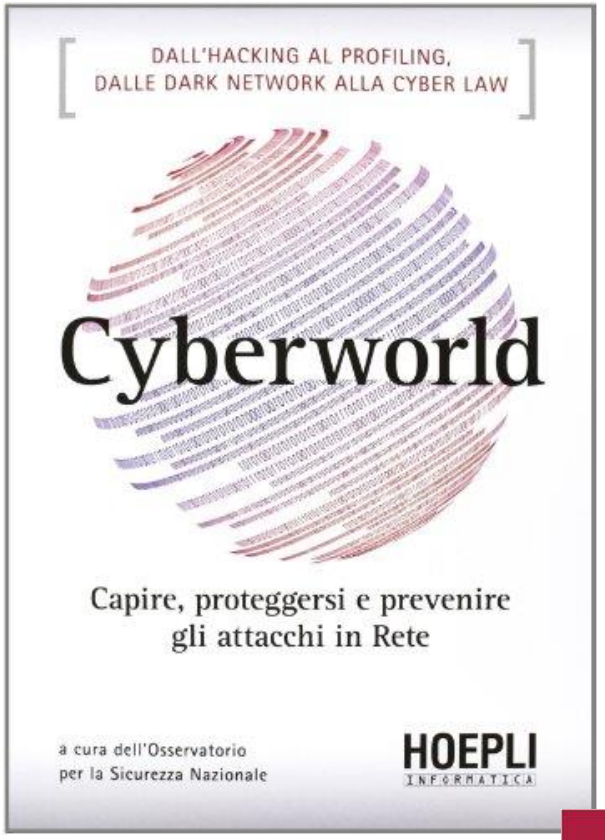
- Lo scorso **Ottobre 2013** è stato il mese dell'**European Cyber Security Month** (ECSM): quante «persone comuni» **ne erano al corrente**?
- Quest'anno l'Italia sta facendo un **ottimo lavoro grazie al CLUSIT**: 25 eventi nel mese di Ottobre!!!!!

- Però, dallo scoppio dello scandalo «Datagate» non ho assistito a **nessuna trasmissione TV** che lo abbia trattato, **almeno come tema centrale**: perché?
  - La mia (forte) **preoccupazione** è che il **Datagate abbia «dato il via» ad uno scenario da Far West**, privo di regole e dove «**tutti sono contro tutti**».

Conclusioni (in italiano)

- **Il mondo in cui viviamo oggi è drasticamente cambiato: è il caso che ce ne accorgiamo!**
- ***Ci fidiamo ancora "troppo" degli altri (free wifi, Big G, FB, Vendors / NSA, etc..)***
- ***Non consideriamo il valore («oro») delle nostre informazioni;***
- ***la Comunità Europea DEVE fare qualcosa;***
  - ***Il Parlamento italiano anche!***
- ***Le leggi, le normative e le Regole di Ingaggio internazionali nel mondo «cyber» vanno riviste;***
  - ***La «privacy» ce la siamo già giocata, molto tempo fa ☹***
- ***… contro i poteri oscuri come la NSA non possiamo ovviamente fare molto…ma si sono presi una bella mazzata!***
- ***Siamo (davvero) vicini ad un punto di non ritorno.***

Books you (really) should read



DOYO: Print your favourite sticker! ☺

DOYO: Print your sticker! ☺

DOYO: Print your sticker! ☺

DOYO: Print your sticker! ☺

Reading Room /1

(Presentazione pubblica) **The commercialization of Digital Spying**, Morgan Marquis-Boire, Claudio Guarnieri, Bill Marczak, John Scott-Railton, Citizen Lab, Canada Center for Global Security Studies, Munk School of Global Affairs (University of Toronto), 2013

No Place to Hide: Edward Snowden, the NSA and Surveillance State, Glenn Greenwald, Penguin Books, 2014

Grazie Mr. Snowden, Fabio Chiusi, edizioni ValigiaBlu/Messaggero Veneto, 2014

Kingpin, Kevin Poulsen, Hoepli, 2012

Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking, Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009

H.P.P. Questionnaires 2005-2010

Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet, Joseph Menn, Public Affairs, 2010

Stealing the Network: How to 0wn a Continent, (an Identity), (a Shadow) (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to 0wn the Box, (V.A.), Syngress Publishing, 2003

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)

Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

Kevin Poulsen, Serial Hacker, Jonathan Littman, Little & Brown, 1997

Takedown, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997

The Art of Deception, Kevin D. Mitnick & William L. Simon, Wiley, 2002

The Art of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2004

@ Large: the Strange Case of the World's Biggest Internet Invasion, Charles Mann & David Freedman, Touchstone, 1998

Reading Room /2

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is "n3td3v"?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002

Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

Compendio di criminologia, Ponti G., Raffaello Cortina, 1991

Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44

Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Contacts, Q&A

- **Need** something, ‘got **doubts**, wanna **ask me smth**?
  - rc [at] security-brokers [dot] com
  - Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?

Let’s talk at the Round Table!