



(Digital) Democracy and massive-control in the post-Snowden age

Raoul «Nobody» Chiesa
Founder, President, Security Brokers SCpA

DefCamp 5th edition, Bucharest, Romania, November 29th, 2014

Agenda

- * Disclaimer
- * Abstract
- * # whoami
- * The scenario
- * The actors
- * Venezuela
- * Ukraine
- * Privacy and Democracy
- * Conclusions
- * Stickers! 😊
- * Reading Room



Disclaimer



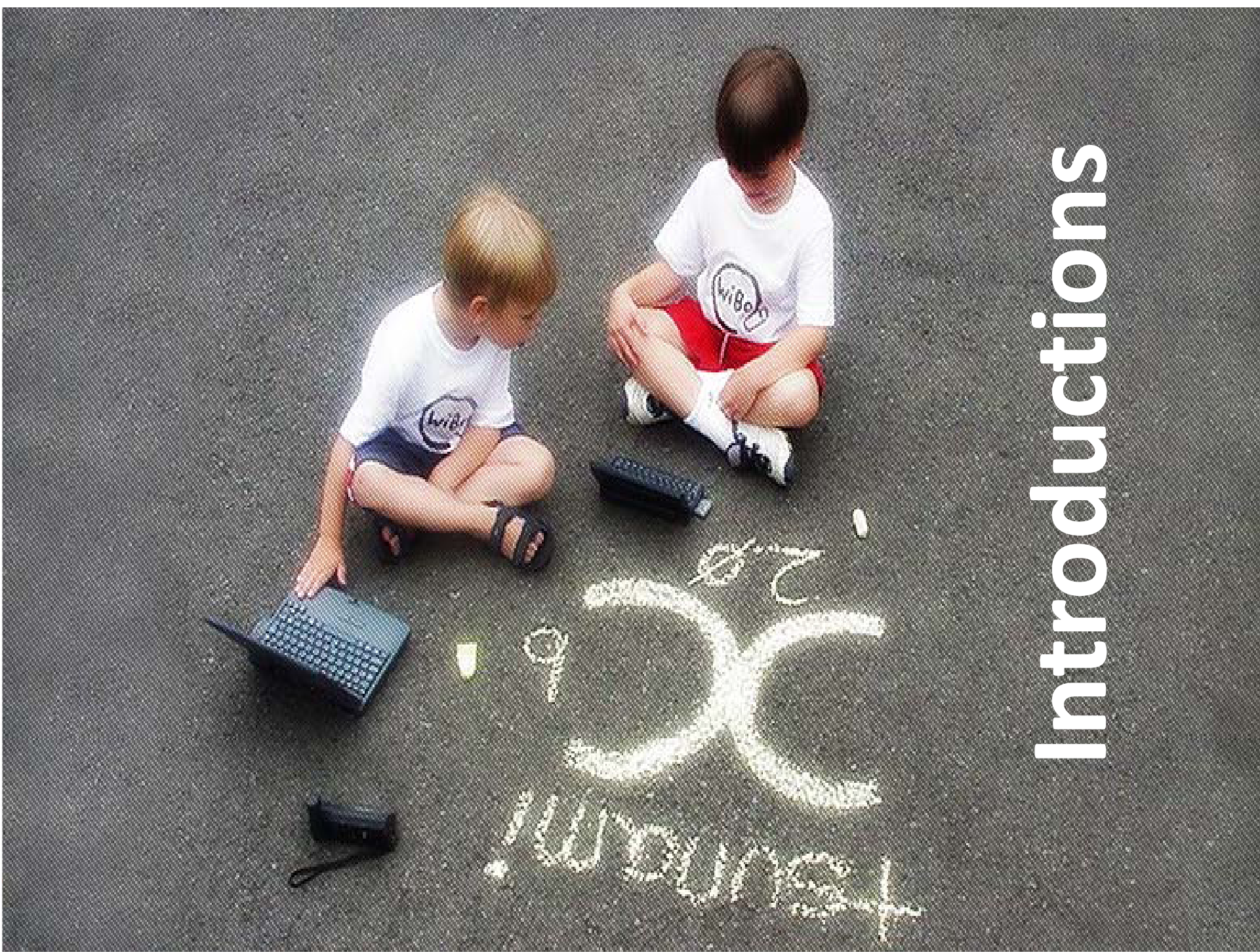
Disclaimer

- 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 local National 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 **its own Associated Partners and Companies**.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.
- **This presentation is not “against” the Government of the United States neither the American people**. Instead, it aims to **seriously highlight** the biggest “affair” happened to the Intelligence community since the Nixon scandal (“Watergate”), and its **impacts towards the concept of democracy itself** in the so-called **Information Age**.

Abstract

- * **Edward 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» (the 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.

Introductions



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 Committee Member @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Former Member, Co-coordinator of the CASD/OSN WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- **Cultural Attachè, APWG European Chapter (APWG.EU)**
- **Supporter at various security communities**



Committed to Wiping Out Internet Scams and Fraud



OWASP

The Open Web Application Security Project



DefCamp 5th edition, Bucharest, Romania, November 29th, 2014

We are (were?) used to this....

Everytime we read about a **data breach**, we do think about the **following scenarios** and **related 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** markets
 - * **State-Sponsored** attacks
 - * **DDoS** powershots
 - *
- * 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 the **United Nations** says (Hacker's Profiling Project):



unieri

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”*

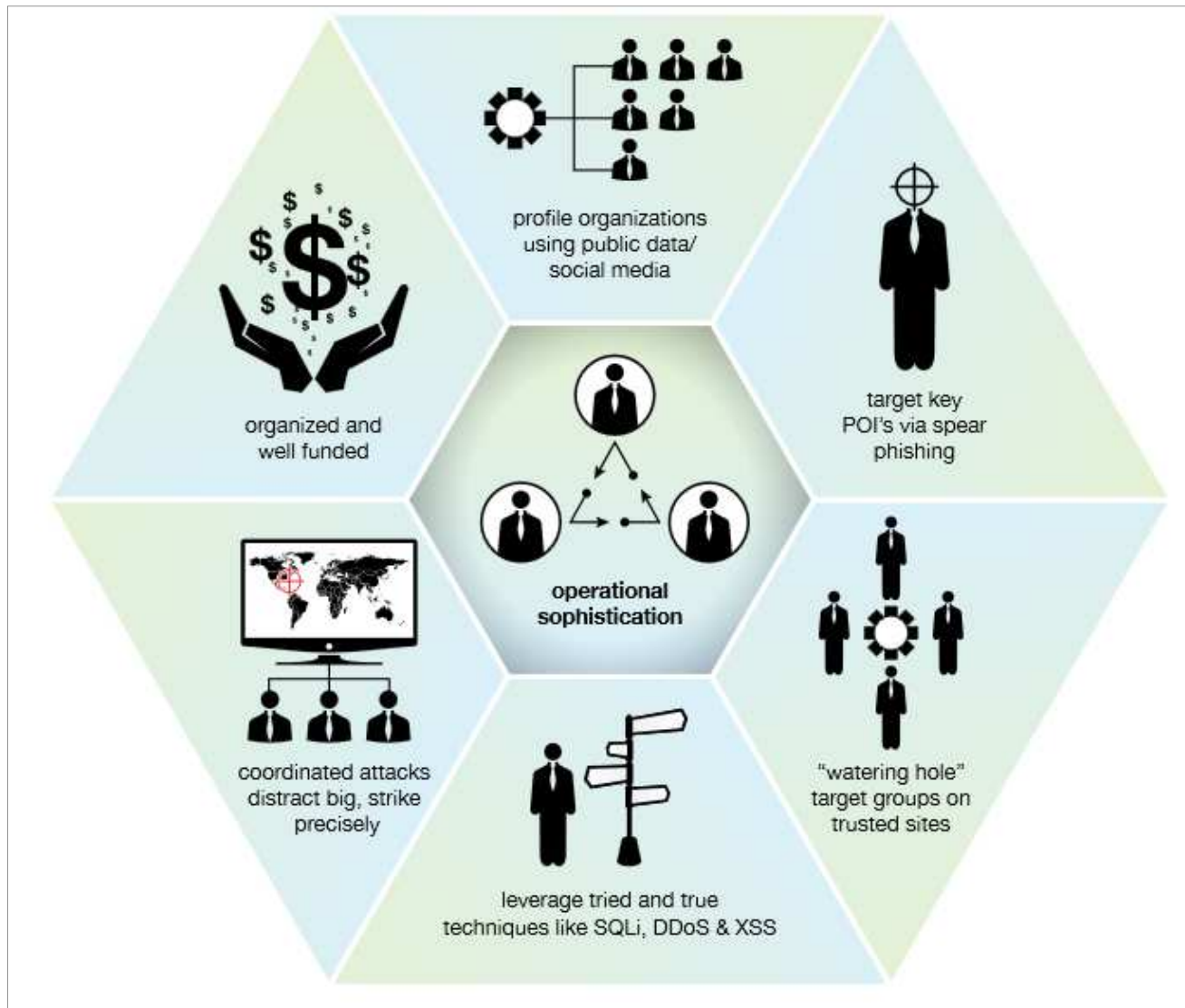
Various sources (UN, USDOJ, INTERPOL, 2011)

*2012 Financial Turnover, estimation: 6-12 \$BLN/year
2013 F.T., estimation: 16-20 \$BLN/year*



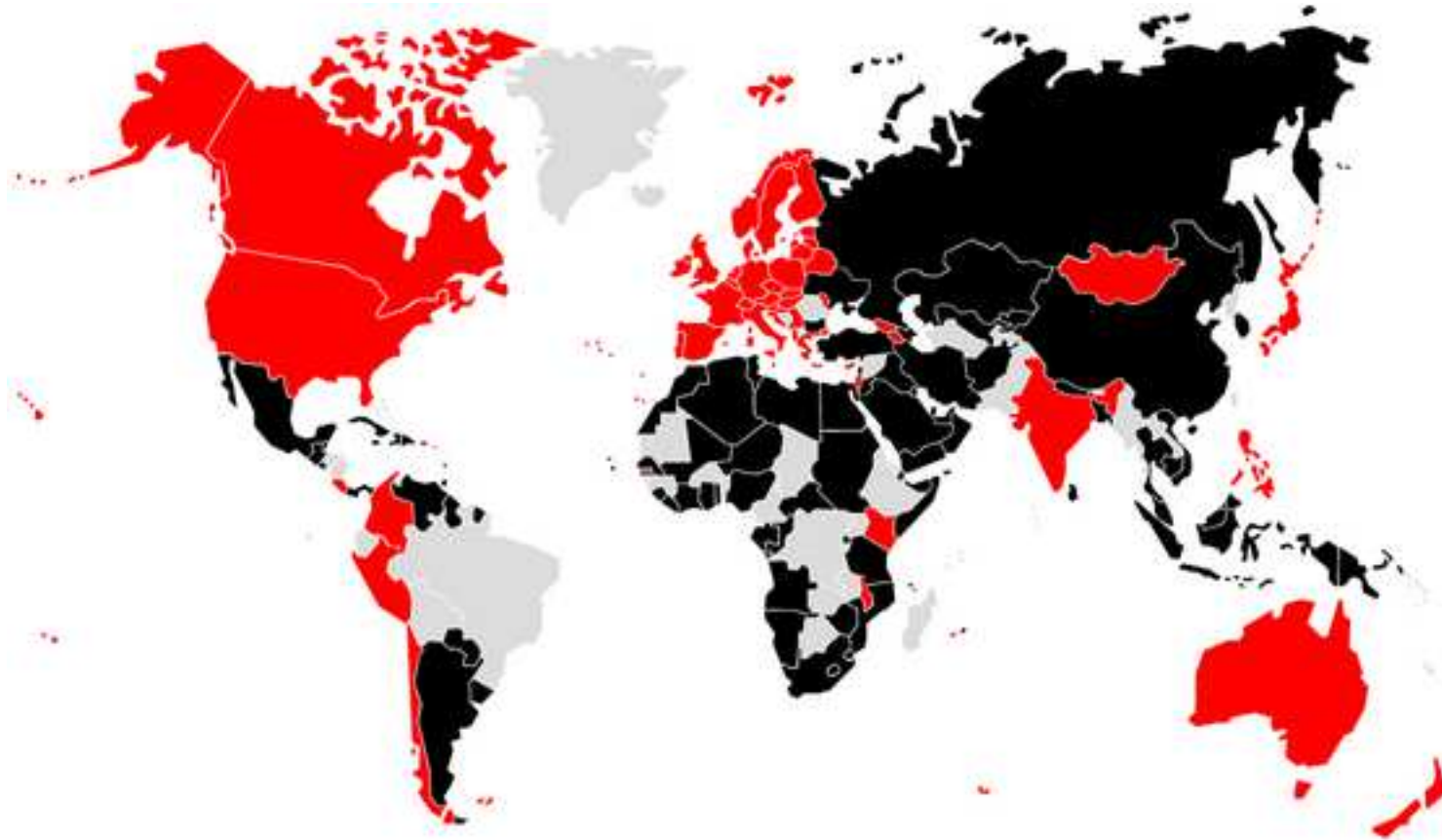
Differences

→ Cybercrime ≠ “hackers”



World

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



Source: Flavia Zappa,
Security Brokers, 2013

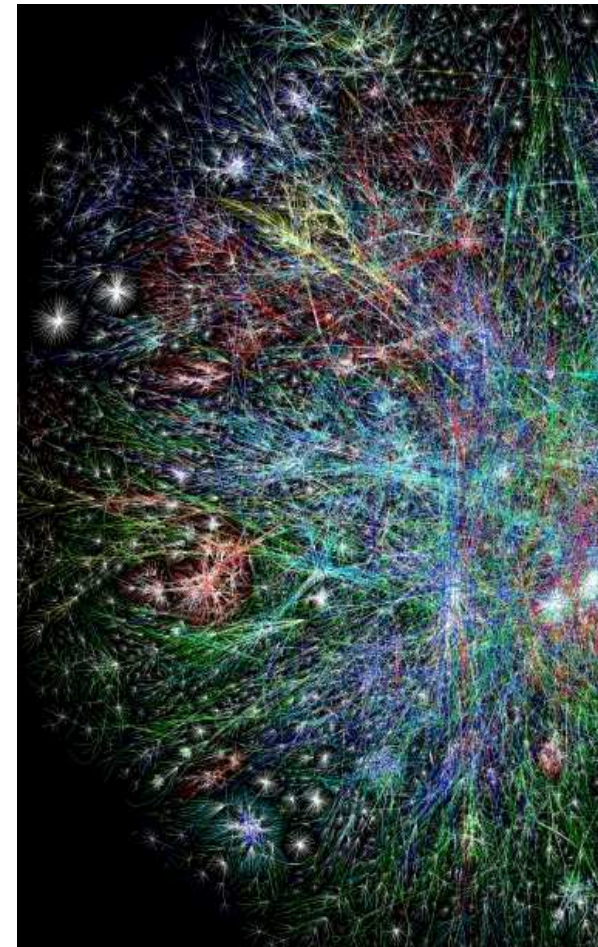
WHAT'S HAPPENING RIGHT NOW

* **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



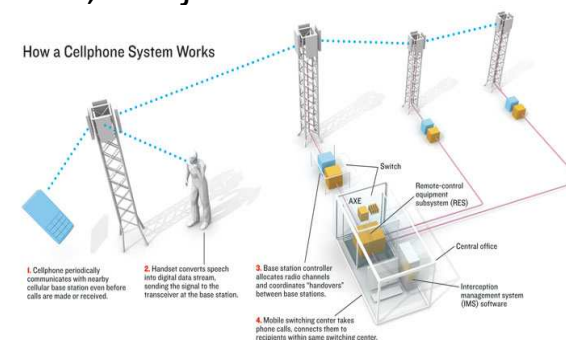
Back in 2005... (?)

→ ...«Privacy?!?»

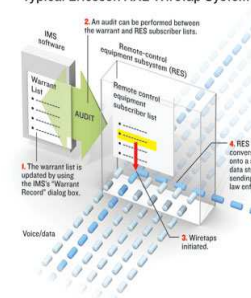
❑ Vodafone Greece 2004 (“The Athens affair”)

- ✓ 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

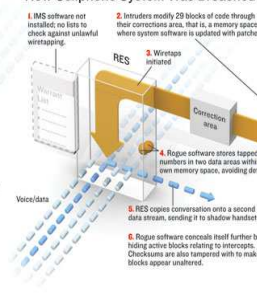
The illegally wiretapped cellphones in the Athens affair included those of the prime minister, his defense and foreign affairs ministers, top military and law enforcement officials, the Greek EU commissioner, activists, and journalists.



Typical Ericsson AXE Wiretap System



How Cellphone System Was Breached



Ahhhhh.... now I get it!

→ ...«Privacy?!?»

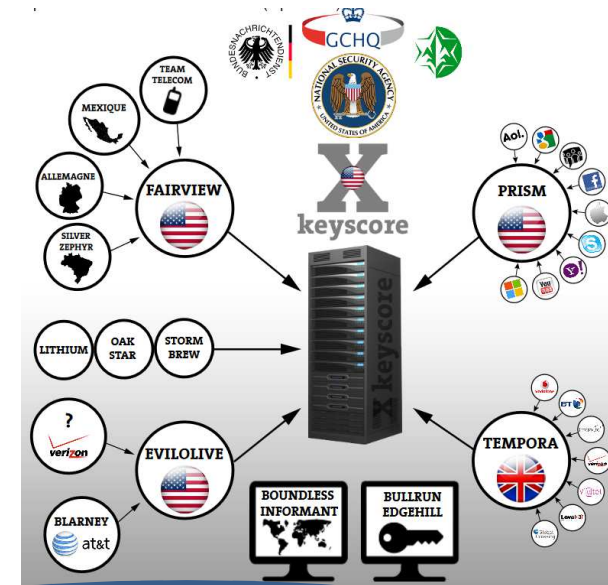
- ❑ PRISM and other secret project's scandals ("the Snowden case")
- ❑ NSA's budgets for black operations revealed
 - <http://rt.com/usa/snowden-leak-black-budget-176/>
 - <http://rt.com/usa/us-hacking-exploits-millions-104/>
 - http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
 - http://www.repubblica.it/tecnologia/2013/08/31/news/sall_ns_a_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



Photo: Santiago Cabezas/Flickr



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



Reuters/Kacper Pempel

DefCamp 5th edition, Bucharest, Romania, November

NSA «black-ops Budget» exposed

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

- ❑ **Targets** - US intelligence agencies highest priorities:
 - ✓ Iran
 - ✓ Russia
 - ✓ China
 - ✓ Afghanistan
 - ✓ North Korea
 - ✓ Syria
 - ✓
- ❑ 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

The Washington Post

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](#)



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 countries -- 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

 Share  2      

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.



DefCamp 5th edition, Bucharest, Romania, November 29th, 2014

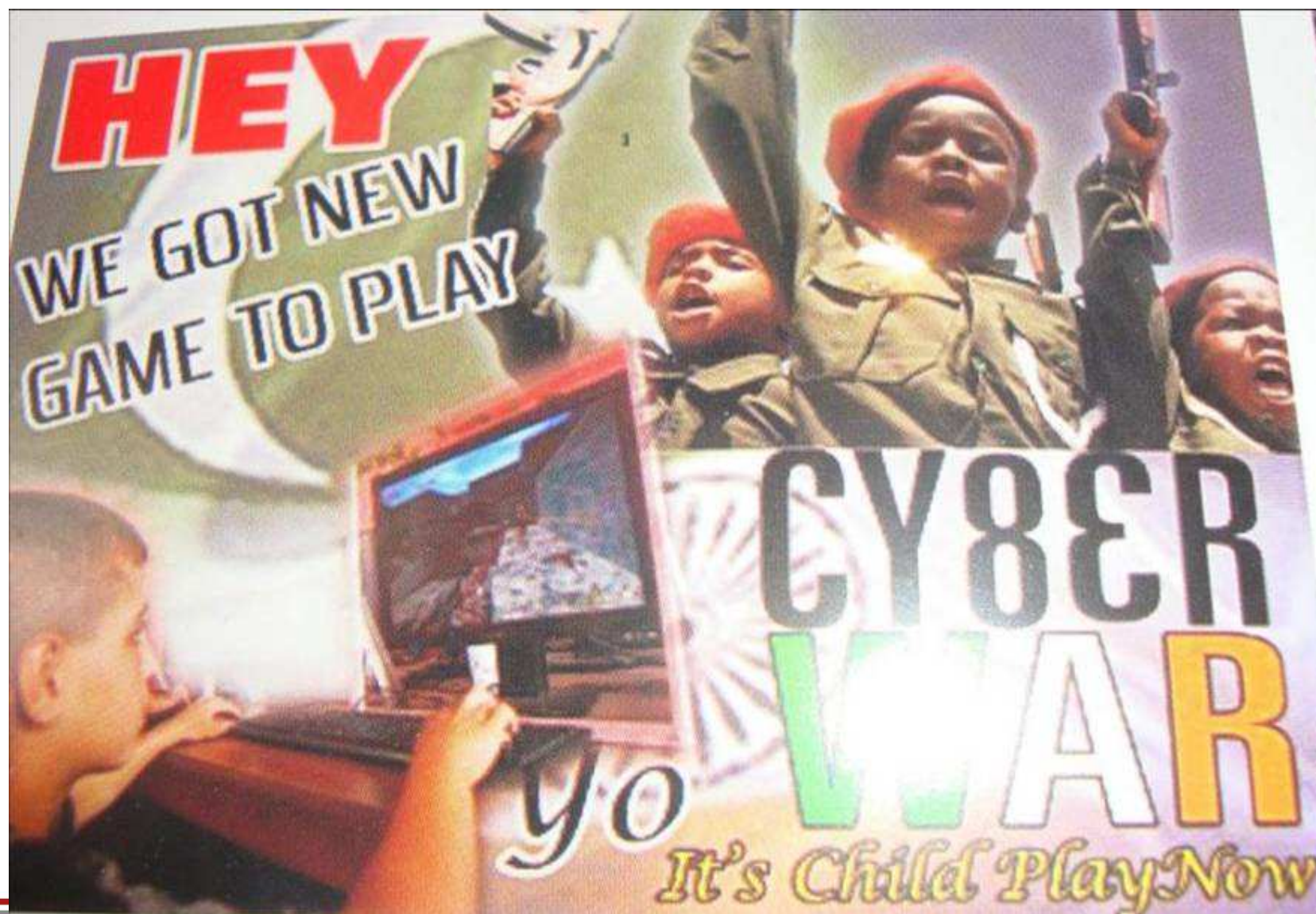


Hmmmmmm.....



Maybe..... 😊





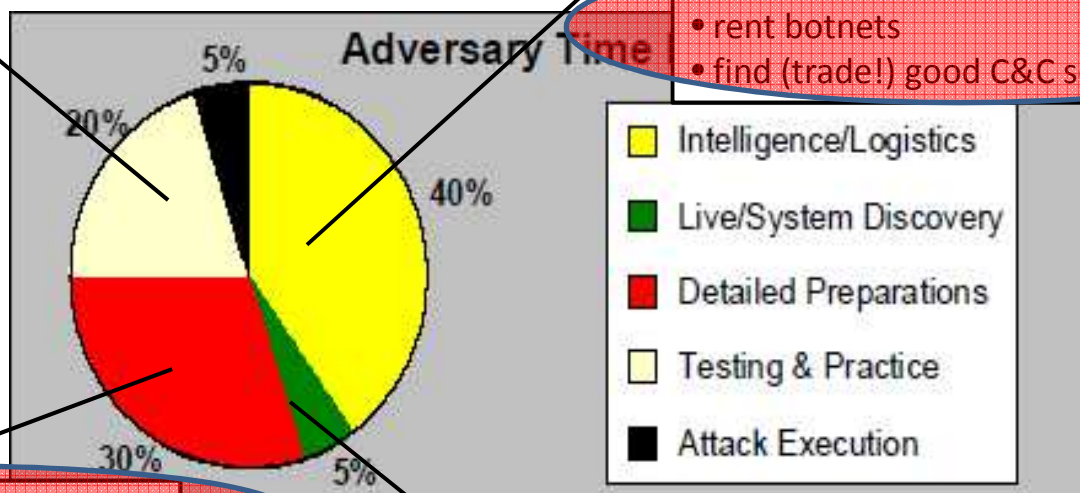
DefCamp 5th edition, Bucharest, Romania, November 29th, 2014



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

SANITIZED

**This slide is not available in the public release
of this presentation.**

**You should have attended DefCamp 5 in order
to see it...**

Scenarios

- * OK, you're smart, you've found the **most ever 133t 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 Phoenixia 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

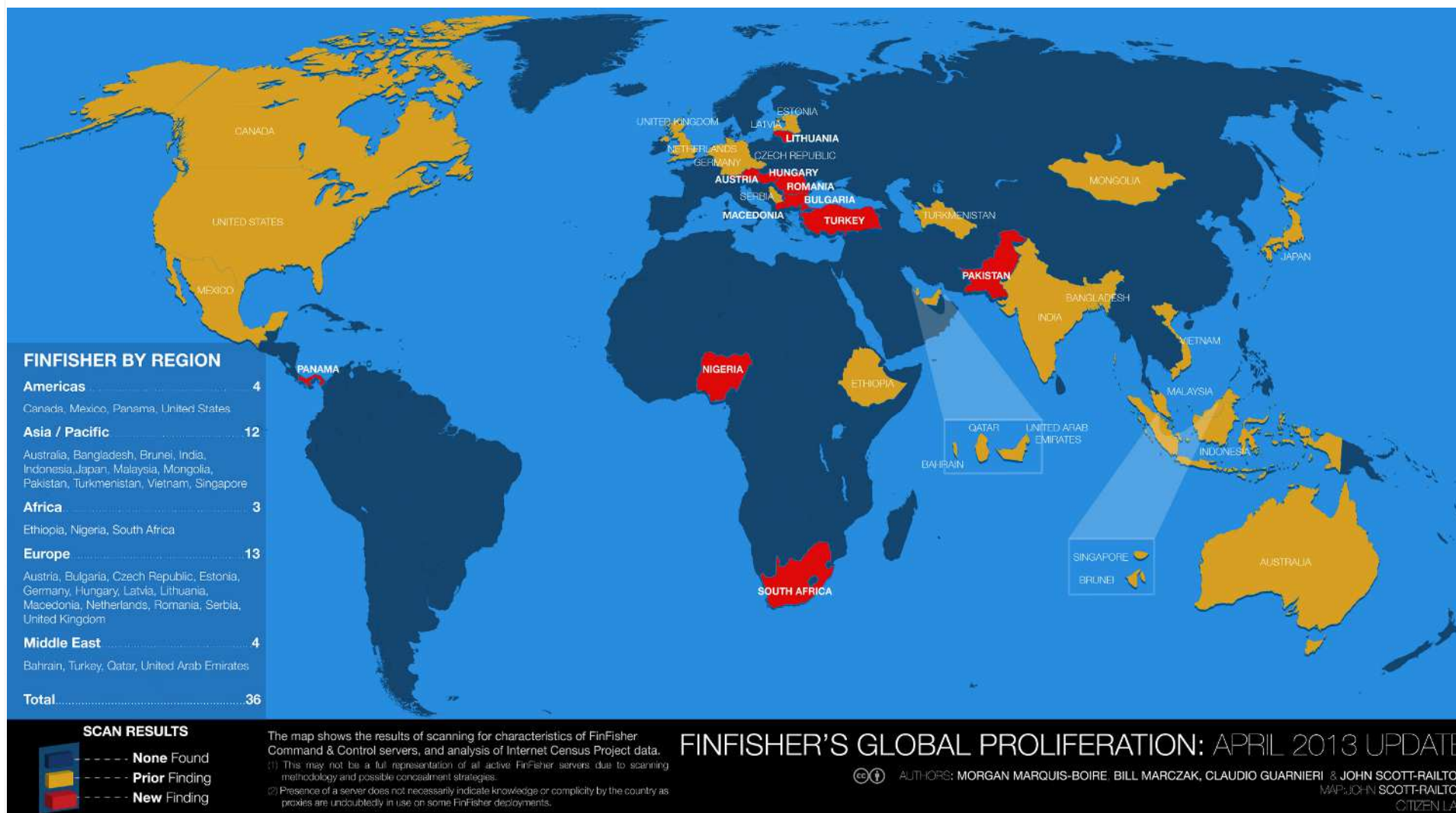
AMERICAS	EUROPE	MIDDLE EAST	AFRICA	ASIA
Mexico Colombia Panama	Hungary Italy Poland	Oman Saudi Arabia UAE	Egypt Ethiopia Morocco Nigeria Sudan	Azerbaijan Kazakhstan Malaysia Thailand South Korea Uzbekistan

CAUSE FOR CONCERN



*World Bank 2012 WGI

Finfisher



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?



DefCamp 5th edition, Bucharest, Romania, November 29th, 2014



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)

Exploitprice_19_JUN_2012.xlsx - Microsoft Excel

S.No.	EXPLOIT NAME	APPLICATION AFFECTED	OS AFFECTED	DEPENDENCY	Price
1	IE 8	IE 8	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	NA	€ 6.000
2	Mozilla Firefox 3.6.16 Exploit	Mozilla firefox 3.6.16	Windows xp, Vista x86 and Windows 7x86	NA	€ 1.200
3	IE 8,9	IE 8,9	Windows xp, Vista x86 and Windows 7x86	NA	€ 3.600
4	IE 6,7,8	IE 6,7,8	Windows xp,Vista x86, Windows 7x86	JRE 1.6 update 26	€ 2.400
5	XLS_2003-2007 all SPs	Microsoft Office Excel 2003 & 2007	Windows xp,Vista x86/x64, Windows 7x86/x64	NA	€ 6.000
6	PDF_9.4	Adobe reader 9.4	Windows xp sp2 and sp3x86	NA	€ 2.400
7	DOC_2007 all service packs	Microsoft Office word 2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	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	windows 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,7x86	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 7x86 x64	NA	€ 2.400
15	JRE & JDK	All Major Browsers	Windows Xp x86, Windows Vista x86, Windows 7x86 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 7x86 x64	NA	€ 3.600
17	JRE & JDK	All Major Browsers	Windows Xp x86, Windows Vista x86, Windows 7x86 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 7x86 x64	NA	€ 2.400
19	VLC media player 1.1.8	VLC media player 1.1.8	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	NA	€ 3.600
20	MS Powerpoint 2007-2010	MS Powerpoint 2007-2010 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86 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
23	.chm file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
24	.hlp file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
25	DOC 2003+2007 all service packs	Microsoft Office word 2003+2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 6.000
26	DOC 2007+2010 all service packs(Double Click)	Microsoft Office word 2007+2010 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 12.000
27	Inpage all version(0day)	Inpage all Versions	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 20.000
28	Flash Player	Flash Player < 10.2.154.27	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400
29	Flash Player	Flash Player < 10.3.181.26	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 3.600
30	Flash Player	Flash Player < 10.3.183.5	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 3.600
31	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 4.800
32	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 4.800
33	Privilege Escalation	Windows Xp x86, Windows Vista x86, Windows 7x86	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400
34	Privilege Escalation	Windows Xp x86, Windows Vista x86, Windows 7x86	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400

* all Versions means Vulnerable one according to CVE

The pricing debate



Top Level Telecommunications

www.electrospaces.net

May 6, 2014

Pictures from inside the German intelligence agency BND

(Updated: June 12, 2014)

The German foreign intelligence service **Bundesnachrichtendienst (BND)** is moving to a brand new headquarters in Berlin. Here we show some unique pictures from inside the former headquarters in the village of Pullach and also give an impression of what the new building looks like.

Unlike for example the United States and the United Kingdom, Germany has no separate agency for collecting Signals Intelligence (SIGINT) - this is done by the BND, and as such this agency is a 3rd Party partner of NSA since 1962 and also participates in the **SIGINT Seniors Europe** or 14-Eyes group.

The former Pullach headquarters

Welcome to this weblog about Top Level Telecommunications!

Here you can read about:

- Signals Intelligence (SIGINT),
- Communications Security (COMSEC),
- Information Classification,

and also about the equipment, from past and present, which make that civilian and military leaders can communicate in order to fulfill their duties.

The main focus will be on the United States and its National Security Agency (NSA), but attention will also be paid to other countries and subjects.

Any comments, additions, corrections, questions or suggestions will be very appreciated! There's no login or registration required for commenting.

http://www.theregister.co.uk/2014/11/11/german_spooks_want_millions_to_buy_0day_vulns/

The pricing debate

German spies want millions of Euros to buy zero-day code holes

Because once we own them, nobody else can ... oh, wait

By Richard Chirgwin, 11 Nov 2014 [Follow](#) 2,707 followers

8

[Adaptable System Recovery \(ASR\) for Linux virtual machines](#)

Germany's spooks have come under fire for reportedly seeking funds to find bugs – not to fix them, but to hoard them.

RELATED STORIES

'Tech giants who encrypt comms are unwittingly aiding terrorists', claims ex-Home Sec Blunkett

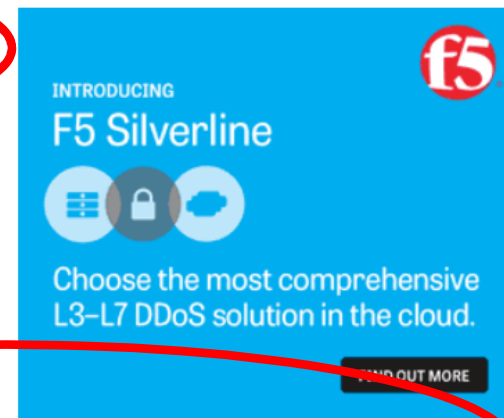
If you're suing the UK govt, Brit spies will snoop on your briefs

Ex-NSA lawyer warns Google, Apple: IMPENETRABLE RIM ruined BlackBerry

According to *The Süddeutsche Zeitung*, the country's BND – its federal intelligence service – wants €300 million in funding for what it calls the [Strategic Technical Initiative](#). *The Local* says €4.5 million of that will be spent seeking bugs in SSL and HTTPS.

The BND is shopping for zero-day bugs not to fix them, but to exploit them, the report claims, and that's drawn criticism from NGOs, the Pirate Party, and the Chaos Computer Club (CCC). German Pirate Party president Stefan Körner told *The Local* people should fear governments more than cyber-terror.

Körner is also critical of the strategy on the basis that governments shouldn't be helping fund the grey market for security vulnerabilities, a sentiment [echoed](#) by the CCC



INTRODUCING
F5 Silverline

Choose the most comprehensive L3-L7 DDoS solution in the cloud.

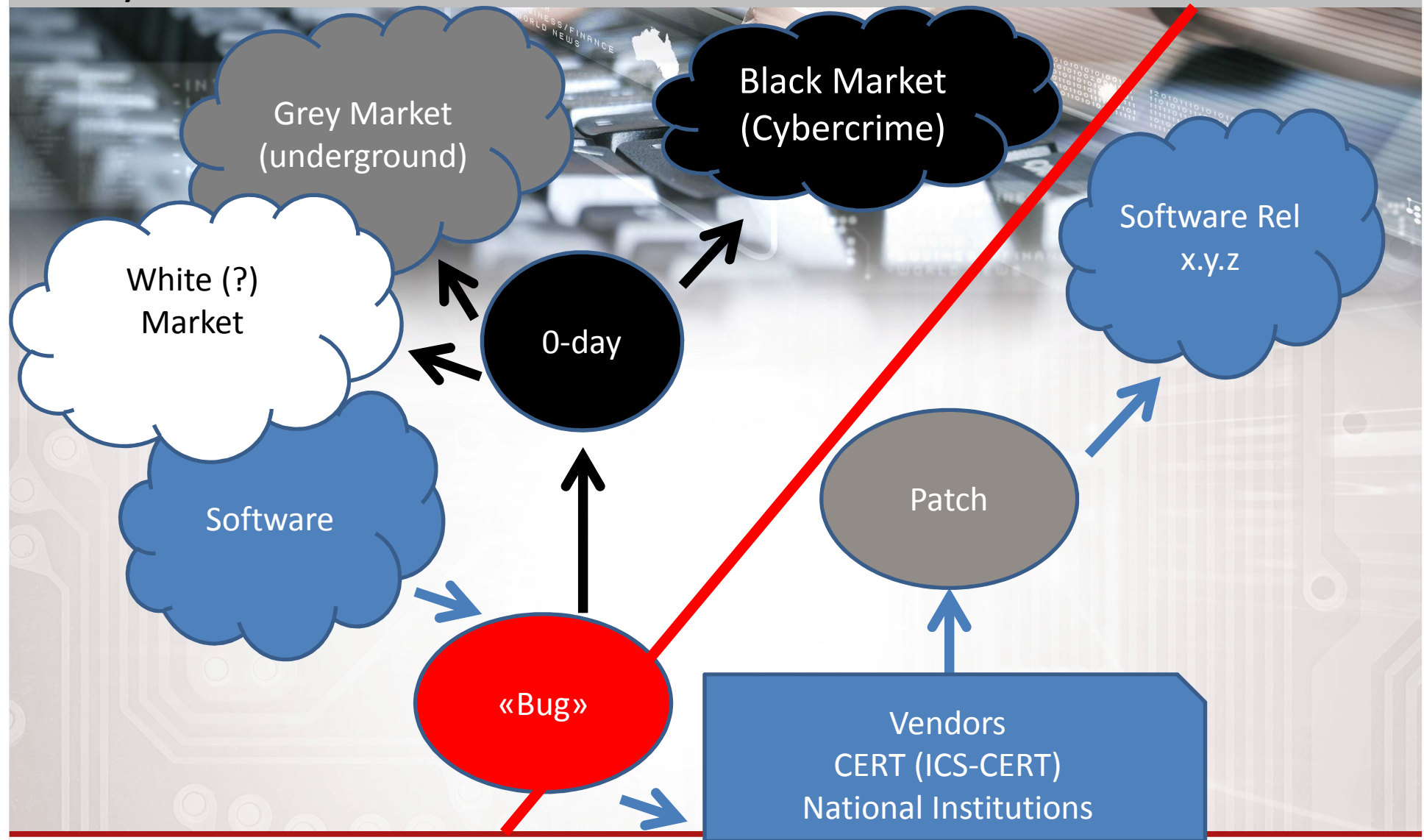
[FIND OUT MORE](#)

http://www.theregister.co.uk/2014/11/11/german_spooks_want_millions_to_buy_0day_vulns/

Black Market?
Grey Market?
White Market?
Prices ranging from thousands to millions?

WTF?!?!?!?

→ 0-day Markets



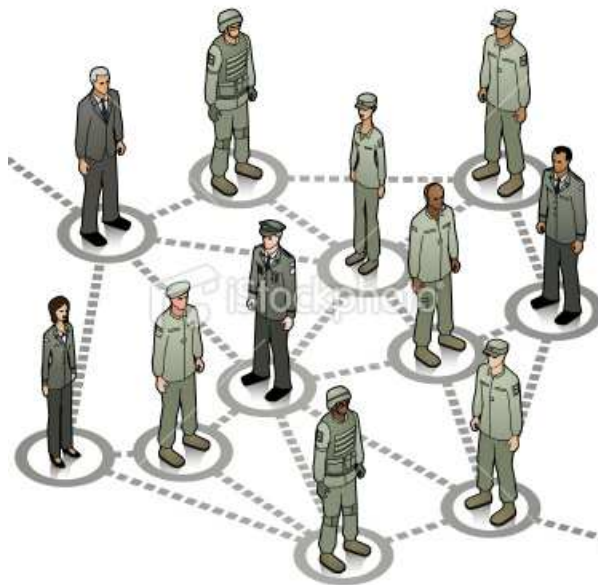
A different (more serious?) approach

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:	Buyer's typology	0-day Exploit code + PoC Cost: Min/Max
	Operating System (OS) Major General Applications (MGA) SCADA-Industrial Automation (SCADA)		
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

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?

- ☐ A couple of years ago 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** (Egypt, Tunisia, Morocco) / **GCC Area** (Gulf Countries)
 - ✓ Think about **IRAN** and **Twitter**
 - ✓ See the **potentialities?**

Hackers in the national cyber security



Csaba Krasznay
IT Security Consultant
Hewlett-Packard Hungary Ltd.



PCWorld article page header. The browser address bar shows the URL: www.pcworld.com/article/117226/feds_seek_a_few_good_hackers.html. The PCWorld navigation bar includes links for News, Reviews, How-To's, Downloads, Shop & Compare, Apps, and Business Center. A search bar is present on the right. Below the navigation bar, there are several promotional banners: a "Magazine" banner for PCWorld Windows Timesavers, a "webroot Personal Security" banner with the tagline "KEEPS BAD STUFF OFF YOUR PC.", and a "holiday Gift guide" banner.

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.

Statistic Hackers Sought

...spinning up business cards and

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

pctools

Hacker 'Mudge' gets DARPA

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

log in | join CNET

Most Visited

Socials

Tools

home | reviews

news

downloads | video

On CHOW: An iPhone app for Thanksgiving!

cnet news

Latest News

CNET River

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

Pelter 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



Speed. Power. Expand.



Powered by Intel

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

Next page guys...

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

[#OpVenezuela] -- [WebHive]

[TARGET]

<http://www.bpvb.gob.ve>

[PETICIONES]

5000

[MENSAJE]

Somos Anonymous, Somos Legion, No perdonamos, No olvidamos, Esperanos!

[STATUS]

SOLICITUDES

5028

LOGROS

3

FALLIDOS

0

STOP!

[Anonymous Venezuela] -- [ANONYMOUS]

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



Apple Google Microsoft Culture Gaming Store

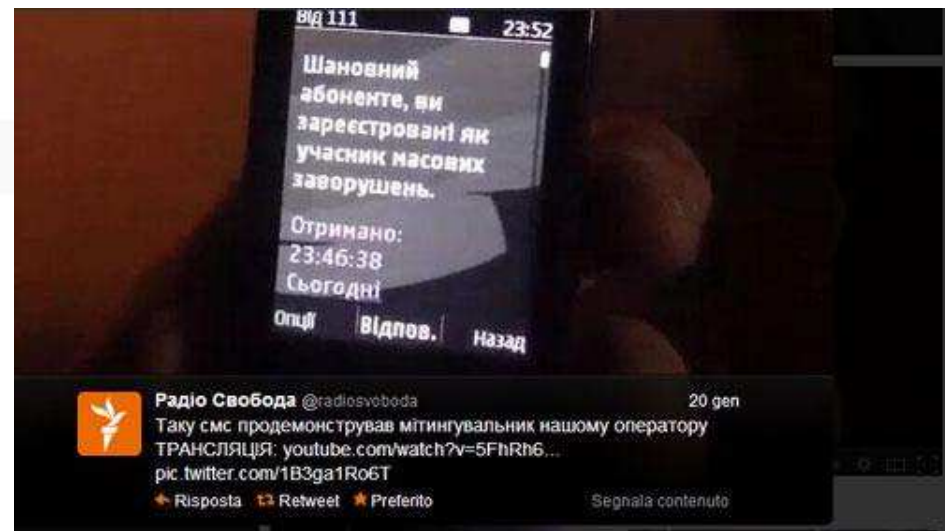
Ukraine using Big Brother like methods to scare protestors.

22 January of 2014 by [technobruus](#)

f Facebook

Twitter

g+ Google



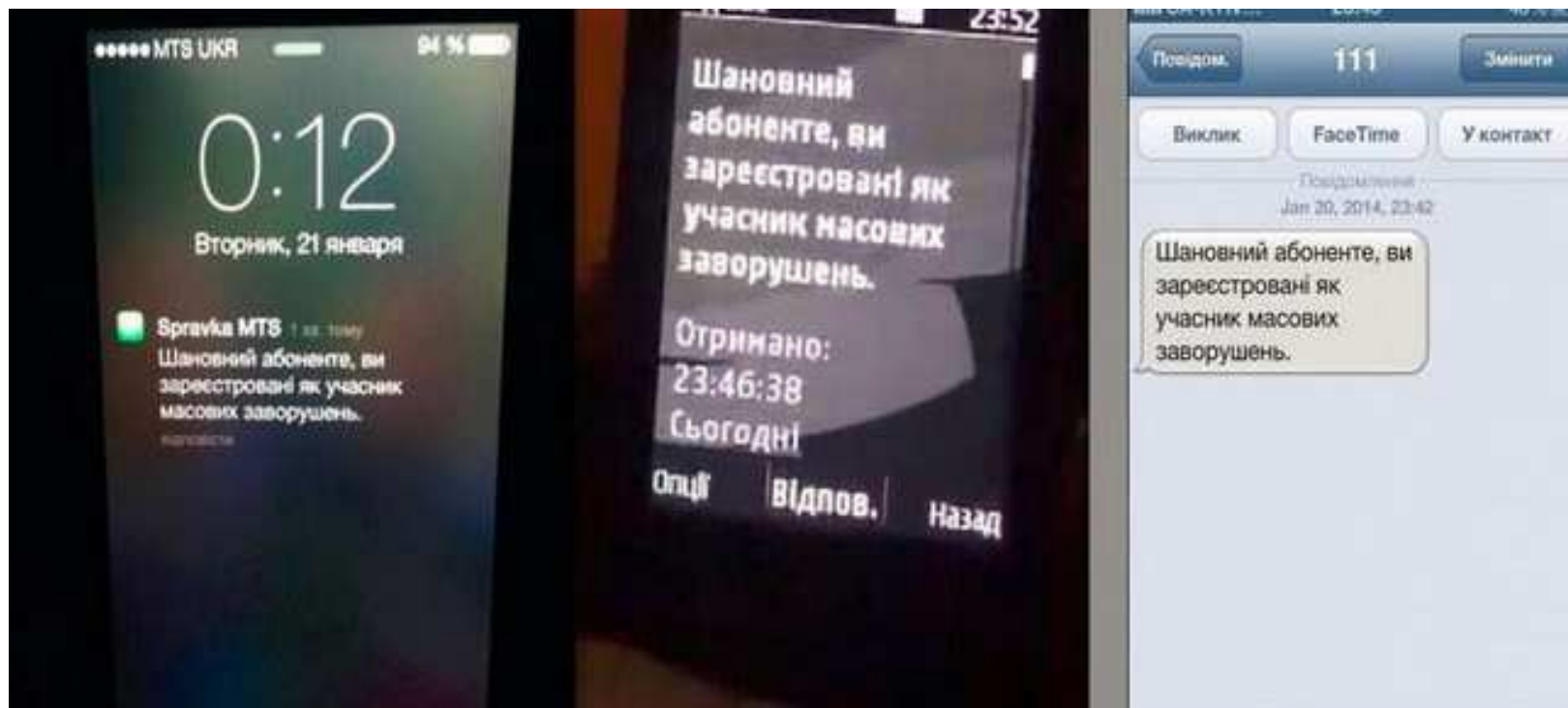
The demonstrations in Ukraine are growing steadily, but now the Ukrainian government have used scary Big Brother like tricks in an attempt to stop the riots.

"Dear recipient, you are registered as a participant in the demonstration."

That is a text that thousands of Ukrainian protesters simultaneously received Tuesday when they took part in a demonstration after the Ukrainian government had outlawed demonstrations. The recipients were gathered in a giant crowd where everyone got the somewhat scary text message from the regime's police force.

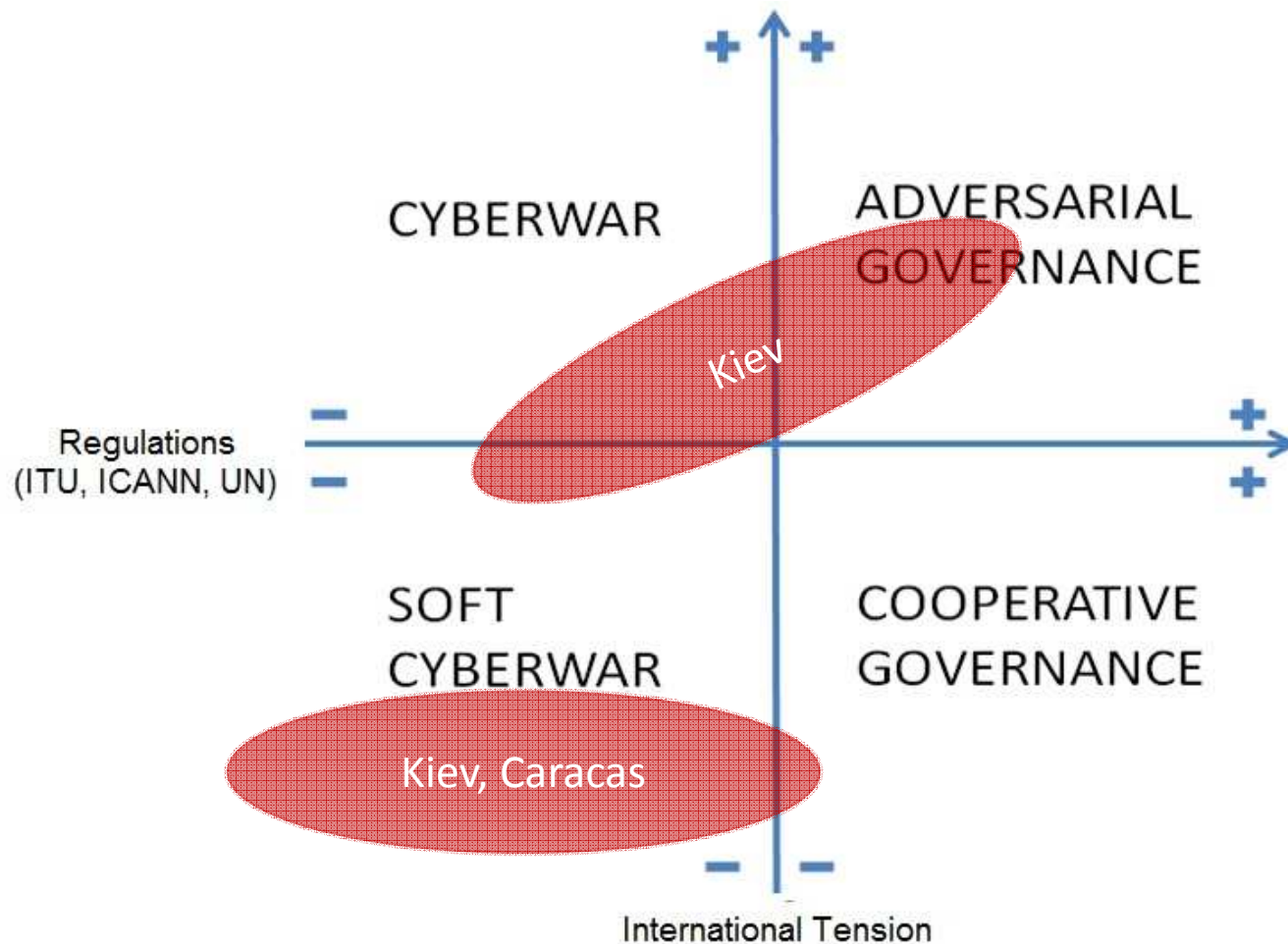
<http://technobruus.com/2014/01/22/ukraine-using-big-brother-like-methods-to-scare-protestors/>

(ab)using Geolocalization



“Dear recipient, you are registered as a participant in the demonstration.”

Evolving scenarios: 2014-2017



So what....?

- Scenarios and happenings which were not «mandatory» including massive information control on the citizens, 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

«Are the Americans ready to **throw away the Constitution**, throw it in the trash, just because **there are terrorists**? And the same thing with the *Bill of Rights* and **all the Amendments**, and the **Universal Declaration of the Human Rights**, the **EU Conventions on Human Rights** and **fundamental freedom**, and the **press freedom**? **Do we really think terrorism is such an existential threat that we're ready to do everything at all?**»

Quoting Mikko /2

«**Privacy is NOT negotiable. It should be built-in to all the systems we use. [...] Surveillance changes the history.** We know this through examples of **corrupted presidents such as Nixon.** Imagine if he would have had the **kind of surveillance tools that are available today.**

Let me **actually quote** the President of Brazil, Miss **Dilma Roussef.** She was **one of the targets** of the **NSA surveillance.** Her emails were read, and she spoke at the **United Nations headquarters,** and she said»:

Hello Miss President.... ☹

(Speech at the United Nations HQ in New York)

*«If here's **no right to privacy**,
there can be **no true freedom of expression and opinion**, and therefore **no effective democracy**.»*

- That's what it's about.
- Privacy is **the building block of our democracies**.
- And to quote a **fellow security reseacher**, Marcus Ranum, he said that «the United States is right now **treating the Internet as it would be treating one of its colonies**.»
- So we are **back to the age of colonization**, and we, the «foreigners» **users of the Internet**, we should **think about Americans as our masters**».



Conclusions

- The world we're living in today has dramatically changed: it's time to wake-up and realize it!
- We still trust too much «third parties»: free wifi, Big G, FB, Vendors / NSA, etc..
- We do not consider the value (gold!) of our information.
- The European Community MUST do something: the domestic Parliaments as well, from Italy to Romania to whatever!
- Laws, Regulations and Rules of Engagement, when it's about «cyber environments», must be revised;
 - We've lost the «privacy» already, a long time ago ☹
- Against those obscure powers such as the NSA we cannot obviously fight too much... even if, they got seriously hit!
- We are (seriously) very close to a no-return point.

DOYO: Print your favourite sticker! 😊

“I don't think a free society is compatible with an organisation like the NSA in its current form.”



DOYO: Print your sticker! 😊



DOYO: Print your sticker! 😊



DOYO: Print your sticker! 😊



Reading Room /1

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, 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 Own a Continent, (an Identity), (a Shadow) (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to Own 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 & Kupfer, (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?

