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

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

Convegno Nazionale e-privacy 2014 – Cagliari, 17-18 Ottobre
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.
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):

<table>
<thead>
<tr>
<th>OFFENDER ID</th>
<th>LONE / GROUP HACKER</th>
<th>TARGET</th>
<th>MOTIVATIONS / PURPOSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>GROUP</td>
<td>End-User</td>
<td>For fashion, It’s “cool” =&gt; to boast and brag</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>GROUP: but they act alone</td>
<td>SME / Specific security flaws</td>
<td>To give vent of their anger / attract mass-media attention</td>
</tr>
<tr>
<td>Cracker</td>
<td>LONE</td>
<td>Business company</td>
<td>To demonstrate their power / attract mass-media attention</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>LONE / GROUP (only for fun)</td>
<td>Vendor / Technology</td>
<td>For curiosity (to learn) and altruistic purposes</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>LONE</td>
<td>On necessity</td>
<td>For curiosity (to learn) =&gt; egoistic purposes</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>LONE</td>
<td>“Symbol” business company / End-User</td>
<td>For profit</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>LONE</td>
<td>Business company / Corporation</td>
<td>For profit</td>
</tr>
<tr>
<td>Government Agent</td>
<td>LONE / GROUP</td>
<td>Government / Suspected Terrorist/Strategic company/Individual</td>
<td>Espionage/Counter-espionage Vulnerability test Activity-monitoring</td>
</tr>
<tr>
<td>Military Hacker</td>
<td>LONE / GROUP</td>
<td>Government / Strategic company</td>
<td>Monitoring / controlling / crashing systems</td>
</tr>
</tbody>
</table>
And, it’s not just «hackers»
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

Breakdown of Russian Cybercriminal Activities

- Online Fraud $942 Million
- C2C Cybercrime to Cybercrime $230 Million
- Spam $830 Million
- Other $168 Million
- DDoS $130 Million

Total Cybercrime Market in US Dollars:

$2.3 billion

$12.5 billion

$4.5 billion
Cybercrime ≠ “hackers”
Geopolitical shift: 2013 - Map of ITU Dubai General Assembly December (red=not signed; black=signed)

Source: Flavia Zappa, Security Brokers, 2013
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€

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://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html](http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html)

The US government might be the biggest hacker in the world
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
  - ......

- Cyber Attacks Unit “GENIE”
- Hacking into foreign systems in order to spy on contents, controlling functions
- [Link](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

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

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.
Convegno Nazionale e-privacy 2014 – Cagliari, 17-18 Ottobre
Hmmmmmm......
Maybe...... 😊
HEY
WE GOT NEW
GAME TO PLAY

CYBER
WAR
It's Child PlayNow

yo
Making “Cyber War”…

- "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

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

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

- Purchase L2/L3 system data

Alexander Klimburg 2012
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
Mexico Colombia Panama
EUROPE
Hungary Italy Poland
MIDDLE EAST
Oman Saudi Arabia UAE
AFRICA
Egypt Nigeria Sudan Morocco
ASIA
Azerbaijan Kazakhstan South Korea Thailand 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

Convegno Nazionale e-privacy 2014 – Cagliari, 17-18 Ottobre
Finfisher

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
  - Eritrea, 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

FINFISHER’S GLOBAL PROLIFERATION: APRIL 2013 UPDATE

Convegno Nazionale e-privacy 2014 – Cagliari, 17-18 Ottobre
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?
The pricing debate

I think all of you remember this:

<table>
<thead>
<tr>
<th>Software</th>
<th>Price Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader</td>
<td>$5,000-$30,000</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>$20,000-$50,000</td>
</tr>
<tr>
<td>Android</td>
<td>$30,000-$60,000</td>
</tr>
<tr>
<td>Flash or Java Browser Plug-ins</td>
<td>$40,000-$100,000</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td>$50,000-$100,000</td>
</tr>
<tr>
<td>Windows</td>
<td>$60,000-$120,000</td>
</tr>
<tr>
<td>Firefox or Safari</td>
<td>$60,000-$150,000</td>
</tr>
<tr>
<td>Chrome or Internet Explorer</td>
<td>$80,000-$200,000</td>
</tr>
<tr>
<td>iOS</td>
<td>$100,000-$250,000</td>
</tr>
</tbody>
</table>

The pricing debate

What about this? (CHEAP but LAME, India’s ones)
Where’s the truth?

What’s the right approach with pricing?
0-day Markets

Black Market (underground)

White (?) Market

Software

«Bug»

Vendors
CERT (ICS-CERT)
National Institutions

Software Rel x.y.z

Patch

Black Market (Cybercrime)
A different (more serious?) approach

<table>
<thead>
<tr>
<th>Public Knowledge of the vulnerability</th>
<th>Buyer’s typology</th>
<th>0-day Exploit code + PoC Cost: Min/Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IS = IT Security companies</td>
<td>IS = IT Security companies</td>
</tr>
<tr>
<td></td>
<td>INT = Intelligence Agencies</td>
<td>INT = Intelligence Agencies</td>
</tr>
<tr>
<td></td>
<td>for Governmental use</td>
<td>for Governmental use</td>
</tr>
<tr>
<td></td>
<td>(National Security protection)</td>
<td>(National Security protection)</td>
</tr>
<tr>
<td></td>
<td>MIL = MoD/related actors for warfare use</td>
<td>MIL = MoD/related actors for warfare use</td>
</tr>
<tr>
<td></td>
<td>OC = Cybercrime</td>
<td>OC = Cybercrime</td>
</tr>
<tr>
<td>Y</td>
<td>IS</td>
<td>10K – 50K USD</td>
</tr>
<tr>
<td>Y</td>
<td>INT</td>
<td>30K – 150K USD</td>
</tr>
<tr>
<td>Y</td>
<td>MIL</td>
<td>50K – 200K USD</td>
</tr>
<tr>
<td>Y</td>
<td>OC</td>
<td>5K – 80K USD</td>
</tr>
<tr>
<td>N</td>
<td>ALL</td>
<td>X2 – X10</td>
</tr>
</tbody>
</table>
A different (more serious?) approach

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

→ «Privacy?!?»

MA MI FACCIA IL PIACERE !!!
"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
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 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.
Hacker 'Mudge' gets DARPA job

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.
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](http://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, Esperamos!

[STATUS]
SOLICITUDES
5028
LOGROS
3
FALLIDOS
0

STOP!

# [Anonymous Venezuela] -- [ANONYMOUS] #
Caracas: hacktivism
The Morning Download: Ukraine Claims Telecom System Hacked

By MICHAEL HICKINS
Editor
(ab)using Geolocalization

Ucraina, il Grande Fratello controlla la piazza via sms?

di Umberto Rapetto | 23 gennaio 2014

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

“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.

- Cyberwar
- Adversarial Governance
- Soft Cyberwar
- Cooperative Governance

Kiev, Caracas

International Tension

Regulations (ITU, ICANN, UN)
So what....?

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

• Government 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)

http://video.ted.com/talk/podcast/2013X/None/MikkoHypponen_2013X-480p.mp4
«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?»
«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»:
(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.»
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 “tropo” 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

- La devianza informatica tra crimini e diritti
- Cyberworld: Capire, proteggersi e prevenire gli attacchi in Rete
- KINGPIN: La vera storia della rapina digitale più incredibile del secolo

Convegno Nazionale e-privacy 2014 – Cagliari, 17-18 Ottobre
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! 😊

Exposing NSA Surveillance Since 2007

The Simpsons
DOYO: Print your sticker! 😊
DOYO: Print your sticker! 😊
(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


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 the Box, (V.A.), Syngress Publishing, 2003


Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quintttner, Harperformans, 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 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
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
Compendio di criminologia, Ponti G., Raffaello Cortina, 1991
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!