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

Raoul «Nobody» Chiesa
Founder, President, Security Brokers SCpA
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.
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 21st Century.
Introductions
Raoul “Nobody” Chiesa

- President, Founder, The Security Brokers
- Co-Founder, Swascan
- Indipendent Special Senior Advisor on Cybercrime @ UNICRI (United Nations Interregional Crime & Justice Research Institute)
- Roster of Experts @ ITU (UN International Telecommunication Union)
- Former PSG Member, ENISA (Permanent Stakeholders Group at European Union Network & Information Security Agency)
- Founder, @ CLUSIT (Italian Information Security Association)

- Founding Member, ECSO (European Organization for Security)
- Board of Directors, ISECOM (Institute for Security & Open Methodologies)
- OSSTMM Key Contributor (Open Source Security Testing Methodology Manual)
- Board of Directors, OWASP Italian Chapter
- Cultural Attaché. Scientific Committee, APWG European Chapter
- Former Board Member, AIIC (Italian Association of Critical Infrastructures)
- 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 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 20 years, the concept of «attacker» has dramatically changed.

Also, the **concept** of a «secure systems» as itself, it just doesn’t exist anymore (IMHO).

Well, actually, it never existed 😊

- Vulnerabilities brought-in by **vendors**
- **0days** markets
- **State-Sponsored** attacks
- **DDoS** powershots
- Users’ stupidity / ignorance
- Data Breaches + 3rd parties’ ones
- ............

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 has «evolved», somehow...

Here’s what the 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>10-18 years The script boy</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>16-40 years The very specialized and paranoid attacker</td>
<td>LONE</td>
<td>On necessity 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»
Cybercrime

«Cybercrime»... why??

«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
2018 F.T., estimation: 50-70 $BLN/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
Differences

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

Source: Raoul Chiesa, 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.
Ahhhh.... 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)
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

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

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

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.
It took them 9 years...

🌟 But they accomplished it 😊

🌟 Raoul in Vienna, 25-26 SEPT 2019: speaking with the Dutch Police
Hmmmmmm......

Hmmmmmm......
Maybe...... 😊
HEY
WE GOT NEW
GAME TO PLAY

CYBER WARS
It’s Child Play Now
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
Slide NOT public – I’m sorry, you should had attended e-privacy 2019 Autumn Edition in Bari in order to see this one!
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 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 of RCS

21 Suspected Government Users of RCS

21 Suspected Government Users of RCS

21 SUSPECTED GOVERNMENT USERS

AMERICAS
Mexico
Colombia
Panama

EUROPE
Hungary
Italy
Poland

MIDDLE EAST
Oman
Saudi Arabia
UAE

AFRICA
Egypt
Nigeria
Ethiopia
Sudan
Morocco
Azerbaijan
Kazakhstan
South Korea
Thailand

ASIA
Thailand
South Korea

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
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)
The pricing debate

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  

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.

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 Korner told The Local people should fear governments more than cyber-terror.

Korner 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.

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

- Grey Market (underground)
- White (?) Market
- Black Market (Cybercrime)
- Software Rel x.y.z
- Software
- Patch
- «Bug»
- Vendors
  - CERT (ICS-CERT)
  - National Institutions

e-privacy XXVI, Bari 3-4 Ottobre 2019 – Autumn Edition
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></td>
</tr>
<tr>
<td></td>
<td>INT = Intelligence Agencies for Governmental use (National Security protection)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MIL = MoD/related actors for warfare use</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OC = Cybercrime</td>
<td></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>OC = Cybercrime</td>
</tr>
<tr>
<td></td>
<td>Major General Applications (MGA)</td>
<td>INT = Intelligence Agencies for Governmental use (National Security protection)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCADA-Industrial Automation (SCADA)</td>
<td>MIL = MoD/related actors for warfare use</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>OS</td>
<td>OC</td>
<td>40K – 100K</td>
</tr>
<tr>
<td>Y</td>
<td>MGA</td>
<td>INT</td>
<td>100K – 300K</td>
</tr>
<tr>
<td>Y</td>
<td>SCADA</td>
<td>MIL</td>
<td>100K – 300K</td>
</tr>
<tr>
<td>N</td>
<td>OS</td>
<td>MIL</td>
<td>300K – 600K</td>
</tr>
<tr>
<td>N</td>
<td>SCADA</td>
<td>MIL</td>
<td>400K – 1M</td>
</tr>
</tbody>
</table>
"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
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?
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.
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...
Next page guys...
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, Esperamos!

[STATUS]
SOLICITUDES
5028
LOGROS
3
FALLIDOS
0

STOP!

# [Anonymous Venezuela] -- [ANONYMOUS] #
Caracas2 (2018-2019)

Out of fuel (!)
Blackouts all around the country
People dead ‘cause no electricity in hospitals
WTF....!!
The Morning Download: Ukraine Claims Telecom System Hacked

By MICHAEL HICKINS

Editor
Ukraine using Big Brother like methods to scare protestors.

22 January of 2014 by technobruus

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 protestors 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.

“(ab)using Geolocalization

“Dear recipient, you are registered as a participant in the demonstration.”
Massive Interception Program
Even worse as it seems...

Dubai, Abu Dhabi
“start-ups” con 10/15 MLN di budget (!)

(Tentative) SSL Certification Authority (!)
Italian people involved
Former NSA actors involved
INSIDE THE UAE’S SECRET HACKING TEAM OF AMERICAN MERCENARIES

Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy — dissidents, rival leaders and journalists.

BY CHRISTOPHER BING • JOEL SCHECTMAN
FILED JAN. 30, 2019 • WASHINGTON
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)

http://video.ted.com/talk/podcast/2013X/None/MikkoHypponen_2013X-480p.mp4
«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?»
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 researcher, Marcus Ranum, he said that «the United States is right know 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.»
■ 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 any Member States in EU, to whateve, wherever!!

■ 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 have been hit much hard!

■ We are very close to a no-return point, seriously.
“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! 😊

The NSA
The only part of government that actually listens.
DOYO: Print your sticker! 😊
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


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 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 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

Thanks for your attention!

QUESTIONS?