Information Warfare & Cyberwar: What’s the Story Morning Glory?

Raoul «Nobody» Chiesa
Founder, Partner, The Security Brokers
Principal, CyberDefcon Ltd.
Partner, TSTF

Security Brokers
Global Cybersecurity Defense Services

CyberDefcon
Telecom Security Task Force
This is the Agenda!

- The speaker
- Scenarios
  - What’s outta there?
  - Definitions w/ a plausible case study/scenario
- Nation’s worldwide status
  - Hot players (countries)
  - Hot players (privatization)
- Building your own Cyber Army
  - General model
  - Business model
  - Operating model
  - Costs analysis
  - Attack Operations….opsss! I mean «Offensive Behaviour! - Costs & Timeframes
- A (theoretical?) case study – Airports all over the world!
- Conclusions
- Credits, Contacts, Q&A
The views expressed are those of the author(s) and speaker(s) and do not necessarily reflect the views of UNICRI, ENISA and its PSG, nor the companies and security communities I’m working at and/or supporting.

This presentation does not have the goal to stimulate your minds into doing nasty and/or illegal actions; its goal is indeed to stimulate the audience to understand what’s happening all over, identify the actors and the players VS the hacking community.

Thank you and....enjoy this talk 😊
Raoul Chiesa

- Founder, Partner, **Security Brokers**
- Principal, **CyberDefcon** UK
- Senior Advisor on Cybercrime @ UNICRI (United Nations Interregional Crime & Justice Research Institute)
- PSG Member @ ENISA (Permanent Stakeholders Group, European Network & Information Security Agency)
- Founder, Member of the Steering Committee and Technical Board, **CLUSIT, Italian Information Security Association**
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- **Coordinator of the «Cyber World» WG** @ Italian MoD (CASD/OSN)
- Founder, Owner, @ Mediaservice.net
Scenarios

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
"... attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."

Sun Tzu: “The Art of War”, 350 BCE

"There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind."

Napoleon Bonaparte in Moscow, 1812
«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

Source: Group IB Report 2011

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions...

Cybercrime is...?

No clear actors...

Cyber – Crime/war/terrorism ?

No common components?
Nevertheless, (cyber-)lawyers looks to live one step ahead (WOW!) in this case.

Lawyer Stefano Mele has been the very first one in the world to give a jurisprudential definition of “cyber weapon”:

“A device or any set of computer instructions intended to unlawfully damage a system acting as a critical infrastructure, its information, the data or programs therein contained or thereto relevant, or even intended to facilitate the interruption, total or partial, or alteration of its operation.”

Cybercrime is still very much a problem and of prime important for the LE community.

  - Though not the focal point of my talk!

“Cyberwar” is often confusing and contradictory. Despite being a term I really don’t like.

  - NOTE: When we use the suffix, "-war" appended to "cyber", we do not mean to use that term lightly or belittle the toll it can take on humanity. This will be echoed again and again in this talk.

We are also not referring to kids defacing public-facing websites (on one end) or to forcing entire national power grids offline (on the other extreme end of the spectrum).

  - ... though that second one is at least theoretically possible, focusing exclusively on that stuff is a red herring as you will see (remember the “Brazil hacks”?)

So what is “cyberwar”? Is it the use of networking on the conventional battlefield ("Network-centric warfare")? Is it espionage and possibly sabotage on an adversary's infrastructure? Is it sabotage directed at an adversary's economic infrastructure?

  - Why does so much "cyberwar" discussed in the media look a lot like espionage and spycraft?
Before “cyberwar”, there was **cybercrime**.

But before “cybercrime”, there was **straight-up hacking**.

- **1980's** - independent actors, hacking is very much on the fringe and motivated, for the most part, by curiosity and egoism.

- **1990's** - still "independent actors" though **serious cybercrime and online fraud** begins to appear. "Cyberwar" was **more of a joke** (or, it was **poorly conceptualized**); in practice it seemed to have been limited to Indian and Pakistani teenagers defacing public and non-critical websites of the opposing country ("Moonlight Maze" incident of 1998 being a possible exception, though the jury's still out on that one).
Back to the 80’s...

Introductions

Scenarios

WW Status

Building! (OyO)

Conclusions

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
The first worldwide-known case about Soviet Union (KGB) hacking into US defense contractors and critical Military and Government infrastructures, using CCC’s hackers Hagbard and Pengo.

- Defense Contractor McLean, VA
- JPL – Jet Propulsion Labs, Pasadena, CA
- LBNL – Lawrence Berkeley National Labs, Berkeley, CA
- NCSC – National Computer Security Center
- Anniston Army Depot, Anniston, AL
- Air Force Systems Command Space Division, El Segundo, CA
- OPTIMUS Database, PENTAGON
- Fort Buckner Army Base, JAPAN
- U.S. AIR FORCE, Raimsten, GERMANY
- U.S. NAVY Coastal Systems Computer, Panama City, FL
- U.S. ARMY 24th Infantry, Fort Stewart, GA
- SRI International, Omaha, NB
- U.S. ARMY Darcom Seckenheim, WEST GERMANY

1989: The Cuckoo’s egg by Clifford Stoll

→ Back to the 80’s... Wanna learn more?

Learn more reading the book!
and/or,
Watch this:

http://www.youtube.com/watch?v=EcKxaq1FTac

....and this, from TED:

http://www.youtube.com/watch?v=Gj8IA6xOpSk

(Cliffy, we just LOVE you, all of us! :)

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
Intelligence Elements

- Information / Data
- Subjects / Actors (Persons, Agents, Organizations)
- Correlation, Analysis and Reporting

Intelligence Actions

- Protect
- Obtain
- Improve
- Influence
- Disturb
- Destroy
Lingo aka Terminologies

- **CNA, CND, CNE**
  - Computer Network Attack
  - Computer Network Defense
  - Computer Network Exploit

- **Some good starters, here:**

- **IO = Information Operations**
  - US *dominates* this...
  - Lot of *misunderstanding* and false interpretations
  - A (very very) LOOOOONG list of terms... (I’m sorry for this! 😞)
### Information Operations: Definitions

- **IO** = Information Operations
- **IW** = Information Warfare
- **IA** = Information Assurance
- **C2** = Command and Control
- **C2IS** = Command and Control Information Systems
- **C2W** = Command and Control Warfare
- **C3** = Command, Control, Communication
- **C3I** = Command, Control, Communication and Intelligence
- **C4** = Command, Control, Communication and Computers
- **C4I** = Command, Control, Communication, Computers and Intelligence
- **C4I2** = Command, Control, Communication, Computers, Intelligence and Interoperability
- **C4ISR** = Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
- **C5I** = Command, Control, Communication, Computers, Combat Systems and Intelligence
IO / Information Operations: Definitions

- I = Intelligence
- S&R = Surveillance and Reconnaissance
- RSTA = Reconnaissance, Surveillance and Target Acquisition
- STA = Surveillance and Target Acquisition
- STAR = Surveillance, Target Acquisition and Reconnaissance
- ERSTA = Electro-Optical Reconnaissance, Surveillance and Target Acquisition
- STANO = Surveillance, Target Acquisition and Night Observation
- ISR = Intelligence, Surveillance and Reconnaissance
- ISTAR = Intelligence, Surveillance, Target Acquisition, and Reconnaissance
- SIGINT = Signals Intelligence
- COMINT = Communication Intelligence
- ELINT = Electronic Intelligence
- FISINT = Foreign Instrumentation Signals Intelligence
- OSINT = Open Source Intelligence
- PSYOPS = Psychological Operations
- IMINT = Imagery Intelligence
- MASINT = Measurement Signal Intelligence
- HUMINT = Human Intelligence
- GEOSPATIAL Intelligence = Analysis and Presentation security-relevant Activities
IO / Information Operations: Definitions

- **OPSEC = Operational Security**
- **INFOSEC = Information Security**
- **COMSEC = Communications Security**
- **PHYSSEC = Physical Security (Human, Physical)**
- **HUMSEC = Human Security**
- **SPECSEC = Spectrum Security**

and includes:

- **EMSEC = Emissions Security** (cables “on the air”)
- **ELSEC = Electronic Communications Security**
- **SIGSEC = Signals Security**

- **C-SIGINT = Counter-Signals Intelligence**
- **ECM = Electronic Countermeasures**
- **EMI = Electromagnetic Interference**
- **IBW = Intelligence-based Warfare**
- **IEW = Intelligence and Electronic Warfare**

(Additions welcome, mailto:indianz(a)indianz.ch)
"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
So, what do I see in the next years 😊 LOL!!
<table>
<thead>
<tr>
<th><strong>Introductions</strong></th>
<th><strong>Scenarios</strong></th>
<th><strong>WW Status</strong></th>
<th><strong>Building! (OyO)</strong></th>
<th><strong>Conclusions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profiling «Hackers» (United Nations, UNICRI, HPP V1.0 – 2004-2010)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

http://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/hpp.php

<table>
<thead>
<tr>
<th><strong>OFFENDER ID</strong></th>
<th><strong>LONE / GROUP HACKER</strong></th>
<th><strong>TARGET</strong></th>
<th><strong>MOTIVATIONS / PURPOSES</strong></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>

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
**Non-state proxies and “inadvertent Cyberwar” scenario:**

„During a time of international crisis, a [presumed non-state CNE] proxy network of country A is used to wage a „serious (malicious destruction) cyber-attack“ against country B.“

**How does country B know if:**

a) The attack is conducted with consent of Country A (Cyberwar)

b) The attack is conducted by the proxy network itself without consent of Country A (Cyberterrorism)

c) The attack is conducted by a Country C who has hijacked the proxy network? (False Flag Cyberwar)

© Alexander Klimburg 2012
Back some years ago...

<table>
<thead>
<tr>
<th>Summary of nation-state cyberwarfare capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>China</strong></td>
</tr>
<tr>
<td>Official cyber-warfare doctrine</td>
</tr>
<tr>
<td>Cyberwarfare training</td>
</tr>
<tr>
<td>Cyberwarfare exercises/simulations</td>
</tr>
<tr>
<td>Collaboration with IT industry and/or technical universities</td>
</tr>
<tr>
<td>IT road map</td>
</tr>
<tr>
<td>Information warfare units</td>
</tr>
<tr>
<td>Record of hacking other nations</td>
</tr>
</tbody>
</table>

The official ones – 2012 (Survey from WG «Cyber World», Italian Ministry of Defense, CASD/OSN

Nations with Cyber Warfare (Offensive) Capabilities

<table>
<thead>
<tr>
<th>Country</th>
<th>Cyber warfare Doctrine/Strategy</th>
<th>CW training/Trained Units</th>
<th>CW exercises/simulations</th>
<th>Collaboration w/ IT Industry and/or Technical Universities</th>
<th>Not official Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Belarus</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>North Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Iran</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Israel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Pakistan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Russia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
The official ones – 2012 (Survey from WG «Cyber World», Italian Ministry of Defense, CASD/OSN)

## Nations with Cyber Defense Capabilities / 1

<table>
<thead>
<tr>
<th>Albania 21,30</th>
<th>Cyber warfare Doctrine/Strategy</th>
<th>CW training/Trained Units</th>
<th>CW exercises/simulations</th>
<th>Collaboration w/ IT Industry and/or Technical Universities</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Argentina 21</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Austria 21,24</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Brazil 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bulgaria 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada 5,30</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyprus 21,42</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Korea 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denmark 21,30</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Estonia 21,30</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Philippines 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finland 22</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ghana 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Germany 21,30</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan 21</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jordan 21</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
Nations with Cyber Defense Capabilities / 2

<table>
<thead>
<tr>
<th>Country</th>
<th>Introductions</th>
<th>Scenarios</th>
<th>WW Status</th>
<th>Building! (OyO)</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Latvia</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lithuania</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Poland</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slovak Republic</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Turkey</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The official ones – 2012 (Survey from WG «Cyber World», Italian Ministry of Defense, CASD/OSN)
“Cyberwar” is real, but it might not be what you think;
  - most of what we as a community and the media call "cyberwar" is in fact better defined under the legal umbrella of espionage,
  - BUT (there is always a but) there is growing interest in defining and addressing it (NATO CCDCoE, US-CYBERCOM, etc)... and this is not a bad thing,
  - BUT, as I will illustrate, a lot of the assets and techniques used in (cyber) criminal or (cyber) espionage operations can easily scale upwards to be used within warfare scenarios.
    - Let’s not forget there are alternate means of changing a state’s behaviour beyond “war”: economics, diplomatic issues, informational advantages...

I prefer the term "information operations" as that is what most cases of today refer to, but "cyberwar" gets the attention of both media and financial planners. So be it.
And of course, in true Anglo-Saxon model, private enterprise emerged to fill the void... **prompting a wave of buy-outs and re-alignments:**

**Acquisition of a leading US security testing business for £8.4m**

NCC Group plc (LSE: NCC, “NCC Group” or “the Group”), the international, independent provider of Escrow and Assurance Services, has acquired US-based Matasano Security LLC (Matasano), an independent security research and testing services provider, for a maximum consideration of £8.4m ($13.6m) in cash.

**Highlights**

- Matasano is a leading US security testing services provider with numerous blue chip clients particularly in software, IT, Internet and financial services.
- Provides a range of services to detect security flaws in applications, systems and networks, using penetration testing, reverse engineering and source code review techniques.
- Substantially increases NCC Group’s presence in New York and Chicago and will further enable the Group to provide customers with one stop testing services across US and Europe.
- Consideration of £8.4m - initially £4.2m, then two further payments up to £4.2m in total over next 24 months against performance related targets.
- Immediately earnings enhancing.
- Year to 30 June 2012, Matasano revenue was £5.0m.
- Financed from existing debt facilities and internally generated cash flow.

**$50 Million Series A Investment in Tenable from Accel Partners**

I am extremely pleased to announce that Tenable has received its first institutional round of funding: a $50 million investment from Accel Partners. The investment will help us continue to develop and improve our solutions and improve our customers’ experience.

Tenable celebrates its 10th anniversary this month. During that time, we’ve made Nessus the number one trusted vulnerability scanner in the world with more than 1 million users across 150 countries. We did this though a combination working closely with our community and continually adding improvements to make our users’ lives easier and through our own innovation to push Nessus to do even more than vulnerability assessments. Today, Nessus not only detects vulnerabilities, it finds malware, botnets, credit cards, configurations that will get you hacked or fined and most recently, issues with your iPhone and Android devices.
And of course, in true Anglo-Saxon model, private enterprise emerged to fill the void... **prompting a wave of “lateral movement” of state workers to the private sector:**

Chertoff security firm hires Hayden, three others

By David Hubler  Apr 16, 2009
Retired Air Force Gen. Michael Hayden, formerly director of the Central Intelligence Agency and National Security Agency, is joining the security advisory firm The Chertoff Group as a principal, the firm announced today.

Former NSA & CIA Director Suggests Employing Mercenaries For Cyberwarfare

by Desire Athow  01 August, 2011

One of the architects of US foreign policy under George W. Bush, General Michael Hayden, suggested that the US Government should consider creating a "Digital Blackwater" during an open conversation with Bloomberg's Allan Holmes and several other cybersecurity specialists on stage, during an event called the Aspen Security Forum.
And if that wasn’t enough...

- Boeing Integrated Defense Systems
- Lockheed Martin Corporation
- ManTech International
- KEYW Corporation
- Palantir Technologies
- Science Applications International Corporation (SAIC)
- Northrop Grumman Corporation
- Raytheon Company
- General Dynamics
- NEK Cyber Operations Group
- Thales Group
- BAE Systems
- Finnmeccanica

**And on and on and on...**
### Table 3.7 Fastest-Growing National Cyberwarfare Markets, 2010-2020

<table>
<thead>
<tr>
<th>Country</th>
<th>CAGR (%) 2010-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>21.5</td>
</tr>
<tr>
<td>France</td>
<td>16.5</td>
</tr>
<tr>
<td>UK</td>
<td>16.5</td>
</tr>
<tr>
<td>Australia</td>
<td>15.0</td>
</tr>
<tr>
<td>India</td>
<td>15.0</td>
</tr>
<tr>
<td>S Korea</td>
<td>15.0</td>
</tr>
<tr>
<td>Italy</td>
<td>14.0</td>
</tr>
<tr>
<td>Russia</td>
<td>14.0</td>
</tr>
<tr>
<td>Germany</td>
<td>12.5</td>
</tr>
<tr>
<td>US</td>
<td>12.0</td>
</tr>
<tr>
<td>Canada</td>
<td>10.8</td>
</tr>
<tr>
<td>Japan</td>
<td>10.8</td>
</tr>
<tr>
<td>RoW</td>
<td>10.0</td>
</tr>
</tbody>
</table>

Source: Cyberwarfare Market 2010-2020 by Visiongain
While it remains mostly unspoken, European intelligence agencies also interface with the "security underground" in their pursuit for actionable intelligence, undisclosed vulnerabilities or tactical know-how.

- While they don't have the same degree of control or coordination over their "contractors" as in certain other more centralized countries to the East, the relationships are generally congenial and profitable for both parties.

- If you don’t believe me, at least believe that they rely on the underground for logistical support:

<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 OSX</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>

Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)

**Inside The Exploit Trading Business**

Selling security flaws is a thriving business — and if you do it right, it’s legal too. Here’s what it looks like from the inside.

<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>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>
<tr>
<td>Attribution or Obsfuscation of the Attack(s)</td>
<td>Vulnerability relays on:</td>
<td>Buyer’s typology</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Operating System (OS)</td>
<td>IS = IT Security companies for Governmental use (National Security protection)</td>
</tr>
<tr>
<td></td>
<td>Major General Applications (MGA)</td>
<td>INT = Intelligence Agencies for Governmental use</td>
</tr>
<tr>
<td></td>
<td>SCADA-Industrial Automation (SCADA)</td>
<td>MIL = MoD/related actors for warfare use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OP = Outsourced «Partners»</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OC = Cybercrime</td>
</tr>
<tr>
<td>Y</td>
<td>OS</td>
<td>OP</td>
</tr>
<tr>
<td>Y</td>
<td>MGA</td>
<td>INT</td>
</tr>
<tr>
<td>Y</td>
<td>SCADA</td>
<td>MIL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OP / MIL</td>
</tr>
<tr>
<td>N</td>
<td>OS</td>
<td>OP / MIL</td>
</tr>
<tr>
<td></td>
<td>SCADA</td>
<td>OP / MIL</td>
</tr>
</tbody>
</table>

Outsourced to (Black) OPs
Figure 17: The Dark Side of Connectivity Constellation

- Cyber attacks
- Terrorism
- Massive incident of data fraud or theft
- Massive digital misinformation
- Critical systems failure
- Failure of diplomatic conflict resolution
- Global governance failure

Origin Risk
Increasing capabilities for cyber crime and attacks.

Pathways
Balance-of-power tips as new actors can wage effective interference and disrupt commerce.

Manifestation
The traditional system of global governance is undermined.

Source: World Economic Forum
Figure 41: Framework for Cyber Threats and Responses

Source: World Economic Forum
Building your own Cyber Army
I. Understand, Identify, List, and Own your weapons.
   I. Focus on goals and constrictions. Rules of engagement?

II. Get soldiers to use them.
   I. You don’t need a lot of real hackers, ya know?
   II. Consider «co-sourcing» for focused black ops.

III. Set up specialized units.
   I. Reverse Engineers, Coders, Cryptologists
   II. Telcos, legacy systems & networks, Finance, SCADA & IA, Satellite, Pure Hardware Hackers, Military/IC experts.
   Don’t forget your own Robert Redford as in Spy Game and a SoB... Ah, and the «Lucky Guy»!

IV. Teach them a methodology.
   I. This is up to you.
   II. Pay attention to the Attribution factor (see later).

V. Get more weapons and update them.
   I. Hacking and Underground events, inner-circles & closed loops, black market and underground market, international trading chances.

VI. Think about new scenarios.
   I. While hunting for old stuff...
• Botnet & drone armies
• DDoS
• Trojans & Worms
• Malware

• Server hacking
• Encryption
• Extortion & Ransom
• Man in the Middle

© 2009-2012 Jart Armin, Raoul Chiesa
Introductions  Scenarios  WW Status  Building! (OyO)  Conclusions

→ e-weapons

Black Energy & alike

- Cluster Bomb

Stuxnet-like

- Cruise Missile

© 2009-2012 Jart Armin, Raoul Chiesa
Introductions  Scenarios  WW Status  Building! (OyO)  Conclusions

→ Cluster bomb VS Cruise

**Black Energy**

- Multiple targets, loud and noisy
  - Massive DDoS
  - Loss of digital communication
  - Cloning of state communications
  - Create confusion

**Stuxnet**

- Laser Guided, precision, and stealth
  - Compromise infrastructure
  - Industrial Sabotage
  - Loss of confidence in systems
  - Create confusion

© 2009-2012 Jart Armin, Raoul Chiesa
- Digital Offense capabilities as a key factor for effective digital cyber warfare.
- Provide cyberspace-wide support for civil and military intelligence operations.
- Real world digital attacks are not just “Penetration testing”.
Recruiting “digital soldier” within a State organization is not feasible.

Key and niche knowledge of experienced digital intelligence analysts and hackers are required.

Most attack technologies developed today will became ineffective by 2 years (max).
Concept to *quickly* and *effectively* develop cyber offense capabilities.

Partnership with private security industry to establish “cyber war capabilities”.

Enhance national and foreign *intelligence capabilities* in cyberspace.

Develop cyber armaments and digital weapons for intelligence and military operations.
CWU: Organization

- Strategic Governance Unit
  - Structure Governance
  - Process Engineering
  - Information Management

- Operations Management Unit
  - Cyberoperations Unit
  - Cyberintelligence Unit

- R&D Unit
  - Attack & Defense Methodology Research
  - Toolkit Research

Introductions  Scenarios  WW Status  Building! (OyO)  Conclusions
Setup of organization units capable of:

- Supporting digital attacks for intelligence operations in civil and military environments.
- Providing a continuous up-to-date provisioning of Cyber armaments and Digital weapons.
- Developing strategic and tactical attack methodologies.
- Managing required resources composed of distributed Non-State Actors for global scale digital conflicts.
Introductions  Scenarios  WW Status  Building! (OyO)  Conclusions

→ Cyber Attack «Methodology», from the Military & DoDs Perspective (March 2012)

Gain access
Social engineering
Laptop theft
Manipulated hard- and software and websites
Exploit gaps
Hacking/Scans/brute force

Install
Malware
Viruses
Trojans
Worms

Manipulation and espionage
Theft or manipulation of information
Manipulation of computers

Cyberwar
• Botnets with DDoS attacks
• Website Defacement
• Intrusion of critical infrastructures
• Damage of systems

Source: Saalbach, Cyberwar Methods & Practice

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
→ Cyber Attack «Methodology» (and, counter-attack), from an Hacker’s Perspective

Source: Jim Geovedi, Indonesia
Actor attribution: does it matter?

„The greatest challenge is finding out who is actually launching the attack“.  
Major General Keith B. Alexander,  
Commander US CYBERCOM / NSA, testimony May 8th 2009,  
„Cyberspace as a Warfighting Domain“ – US Congress

„Attribution is not really an issue“.  
Senior DoD official, 2012 Aspen Strategy Group

Attribution:
- tactical level = irrelevant
- operational level = helpful
- strategic level = important
- political (board) level = critical

© Alexander Klimburg 2012
Setting up a proper team

**CYBER TEAM**

Skill & Economical Gaps

Power Outcome

Threat Vulnerability Risks

Information Sharing

Legal Understanding

Enabling Technologies

Situational Awareness

Cyber Risk / Threat picture

IT-Security

Constrains/ Network

Development of secure IT-Infrastructures

Legal aspects of Cyber Security

Intern. / Nat. Regulations, Norms

Exercise/Experimentation

Blue, Red, Yellow Teams

Information / Decision process

Cyber Threat picture

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
Most CNE attacks are non-state, but they are state directed, affiliated, or tolerated … and virtually all of them depend on the non-state for support.

- 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
It's outta there. Now.

Introductions
Scenarios
WW Status
Building! (OyO)
Conclusions

"Information Warfare"

"Information Operations"

"Cyberwarfare"

"Cyberpower"

"Strategic cyber ops"

"Military cyber ops"

CNO
CNA/CNE
CND
OPSEC
EW
PSYOPS
MilDec

Cyber-espionage (CI)

Cyber-Diplomacy

National Crisis Management

Internet Governance

© Alexander Klimburg 2012

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
Cyberwar: a (theoretical) case study

Let’s get creative...

- Ah, so many soft targets...
- How about commercial aviation networks? They are often dual-purpose (useful from an intelligence perspective in peace-time, and relied on as logistical hubs in times of unrest or conflict).
- In the latest time hackers are getting an increasing interest on this topic (see Renderman’s research + other ppl).

SITA is a multinational network linking various players in the air transport sector, namely airports.

- has services for everything from airport management to aircraft in-flight communications and other operational infrastructures.
- operates in over 200 countries!
  - ... the definition of a “target-rich environment”.
  - And how many of them do you think are interconnected with one another? Lateral movement within a wide-area network is trivial...
- often relies upon legacy systems and protocols such as X.25, which are all but forgotten today (see my previous talks at HITB in the past years on X.25 hacking)
Cyberwar: a (theoretical) case study
Cyberwar: a (theoretical) case study

Introductions
Scenarios
WW Status
Building! (OyO)
Conclusions

AIRCOM ACARS

Airline Operations Systems
Airline Commercial Systems
Airline Staff
Access to Passengers via Public email & SMS

SITA Air Transport Industry Messaging

Airport Ecosystem

Fares Data Providers etc.
Global Distribution Systems
Aircraft Manufacturers
Customs/Immigration
MET Offices
Air Traffic Control
Cyberwar: a (theoretical) case study

Scenarios

Hong Kong International Airport
Stockholm-Arlanda Airport

How much tonnage of cargo goes through Frankfurt every day?

What if Frankfurt were shutdown for a day, a week, a month?

How much value is lost? Not a bad ROI for a 100k-500k USD investment...

Even keeping in mind that the goal is constant interruption (not destruction) of a supply chain and major economic hub.

Chicago Airport
Cologne Bonn Airport
Geneva International Airport
Frankfurt am Main Airport

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
• Cyber-Attacks can be used to fit a goal; and in preparation to, during, and after a war. But wars cannot be won only by that. The decisive battle will be still fought with regular forces.

• Nations with high dependence on IT are in need of a central body that collects, analyzes, and assesses all pertinent information from government agencies as well as from private parties.

• No warning - surprising!

• Relative means (compared to conventional attacks) = great impact!

• Immediate effect worldwide!

Traditional Force/Time/Space assessment is not working anymore
Defenders have to protect against all possible channels of attack.

The attackers only have to find one weak point to attack at a time and place of their choice.
Most organizations buy a security suite, perform some quarterly or annual tests and assume they have continuous and flexible monitoring in place, while in reality they improved their security posture from "entirely blind" to "mostly blind".

- So how do you defend against “state-serving adversaries”, “APT” or otherwise very motivated adversaries?

**Step 1:** ASSUME COMPROMISE.

- Cynical but critical.

**Step 2:** Develop robust “threat awareness” or (if applicable) CI procedures.

- “Cyberweapons” and accompanying methodologies are highly fungible and rendered obsolete once disclosed.
- Added value: techniques and methodologies are often re-used for multiple campaigns by the same actors; analyzing the modus operandi can help in attribution over the long term.

**Step 3:** Exchange intelligence with your peers, even internationally.

- Examples: threat intelligence, indicators of compromise & signatures, disclosure of data breaches.
If most of you guys here would **identify your most trusted, motivated and/or skilled friends** from the **local and international hacking scene** (yeah, the very same people you always get drunk with at PH-Neutral, HITB and CONfidence just to mention a few), **let's say 10 of them, YOU WOULD BE IN!**

- Find a **victim** who should «coordinate» them («the g», LOL!!)
- Identify the **Team Leader** (seriously)
- **Get your** «Man at the Havana» (w/ Robert Redford’s style)
- Run a **market survey** (yup...there ARE competitors!!)
  - +120 countries are developing Cyber Warfare capabilities: see “**CyberWarfare Market 2010-2020**” by VisionGain (NOTE: that book costs a BUNCH of money tough!!!! 😑)
- **Jump in!**
But...there’s always a BUT!

- **Pay attention**: it’s a «very weird market» that is **easily disturbed**.
  - As in, an aquarium is easily disturbed by *introduction of a new fish* or *outside disturbance 😊*

- **Be clear**, be «fair»: set up **rules**, respect them.

- **It’s not a game**.
  - **Actors** involved may **betray you** (from all around...)

- **Stay in the white-list**.
Salted Hash — IT security news

About this Blog: IT security news analysis, over easy! Read Bill’s Bio | See Bill’s Posts

Teenage hackers could be our last, best hope

Posted May 22, 2012 to Data Protection | Add a comment

I got an email yesterday asking if teenage hacking is on the rise. At first I balked. Teenage hackers have always been in abundance, so the question seemed stupid to me. Then I remembered something about teens that the SANS Institute’s Alan Paller mentioned at a conference last week.

Let’s start with that press release, which framed the scenario this way:

Is Teenage Hacking On The Rise?

Since the dawn of the personal computer, the words “teenage” and “hacker” have often been inextricably linked.

And classic films such as “Hackers,” “Sneakers” and “WarGames,” —not to mention one of the greatest scenes in pop culture—fit from the game “Capture the Flag”, about young hackers who find themselves in...

Hackers in the national cyber security

Csaba Krasznay
IT Security Consultant
Hewlett-Packard Hungary Ltd.
Your homeland needs you, what do you do?

References

11. http://www.slideshare.net/hackfest/dprkhf

Raoul Chiesa, Ioan Landry - Security Brokers @ HITB 2012 – October 11th, Kuala Lumpur, Malaysia
Kudos to:
- Ioan Landry
- Jart Armin
- Francesca Bosco
- Alexander Klimburg
- Indianz.ch
- Naif
- «Cyber-Lawyer» Dr. Stefano Mele
- Colonel Josef Schroefl, Austria MoD
- Andrea Zapparoli Manzoni

Supporters:
- The HITB Crew
- Dhillon, Belinda, Amy 😊
Raoul «nobody» Chiesa
rc@security-brokers.com
SUBJ: HITB KUL 2012
GPG Key:
http://raoul.EU.org/RaoulChiesa.asc