CYBERCRIME, CYBER ESPIONAGE INFORMATION WARFARE AND «CYBER WAR»: THE FIL ROUGE WHICH CONNECTS THE DOTS

Raoul Chiesa

President, Security Brokers SCpA

Seminar «The role of Cyber Defence to protect and sustain EU economy»
Rome, October 30th, 2014

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**, its **Associates** and **Associated Companies**.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

Agenda

- Introductions
- Cybercrime
  - Scenarios and Actors
- Profiling «Hackers»
- Information Warfare
- Cyber Espionage
- Conclusions
- References

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
- Member, Co-coordinator of the WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè and BoD Member for **APWG.EU**
- **Supporter at various security communities**

First of all

No common spelling…

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?…

❑ In those non English-speaking countries, problems with correctly understanding words and terms **rise up**.

The scenario(s) and the Actors

Crime -> Today

*You got the **information**, you got the **power**..*

Simply put, this happens because the "*information*" can be **transformed at once** into "something else":

1. **Competitive advantage (geo/political, business, personal relationships)**
2. **Sensible/critical information (blackmailing, extorsion)**
3. **Money (Cash-out techniques, Black Market & Underground Economy)**

- … **that's why** all of us we want to "*be secure*".

- It's not by chance that it's named "IS": **Information Security** ☺
  - The **trend** of the «cyber-prefix» is from **very recent years**, tough.

Cybercrime

- **Cybercrime**:

  *"The use of IT tools and telecommunication networks in order to **commit crimes** in **different manners**".*

- **The axiom of the whole model:**

  *"acquiring different types of **data** (information), which can be transformed into **an advantage**."*

- **Key points**:
  - **Virtual** (pyramidal approach, anonimity, C&C, flexible and scalable, moving quickly and rebuilding fast, use of "cross" products and services in different scenarios and different business models)
  - **Transnational**
  - Multi-market (**buyers**)
  - **Differentiating** products and services
  - **Low** "entry-fee"
  - **ROI** /Return of Investment (on each single operation, which means that, exponentially, it can be industrialized)
  - Tax & (cyber) Law **heaven**

Why?

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

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

"2013 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

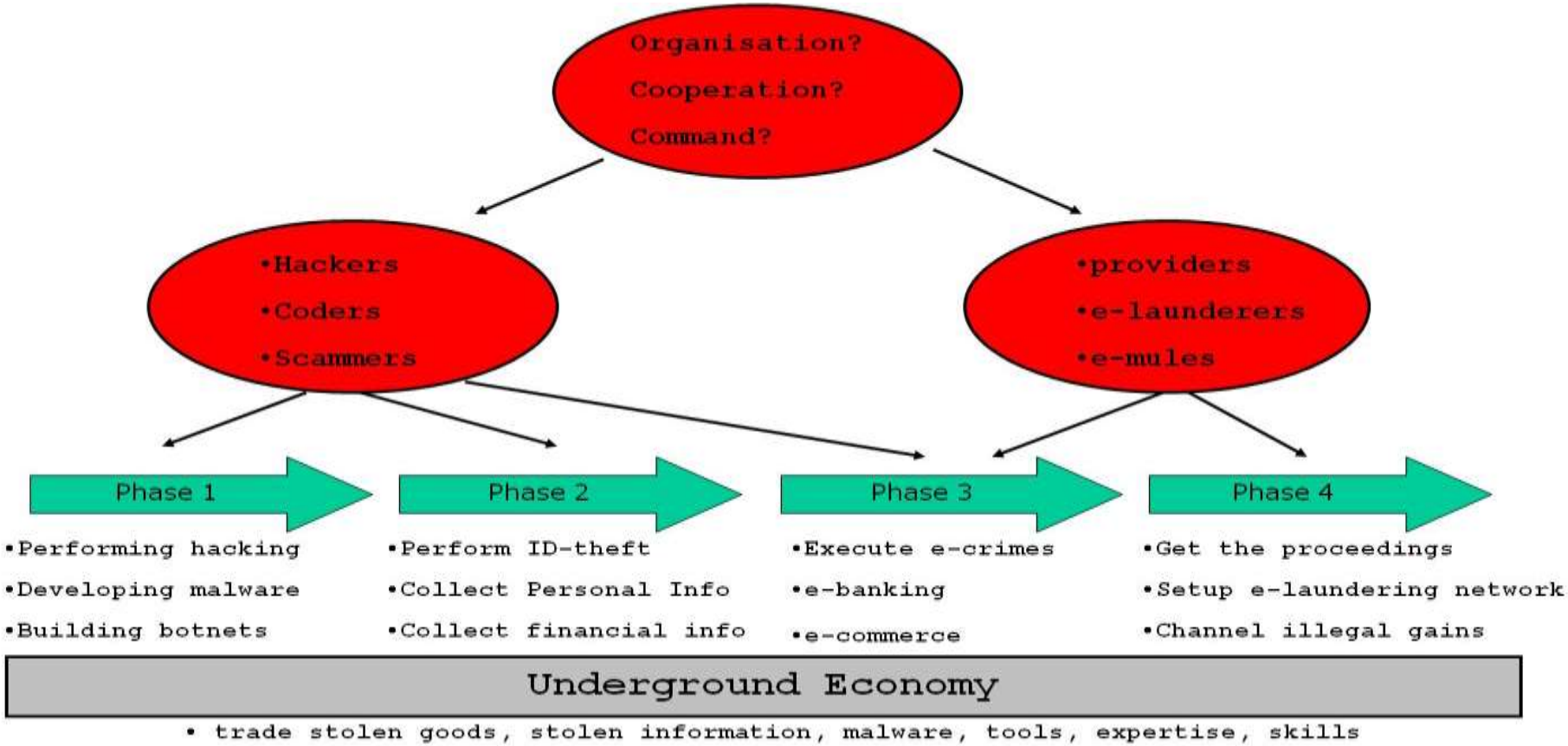
Various sources (UN, USDOJ, INTERPOL, 2013)

Financial Turnover, estimation: 12-18 BLN USD$/year

From Cybercrime to…

- We are speaking about an ecosystem **which is very often underevaluated**: most of times, Cybercrime is the **starting** or **transit point** towards different ecosystems:
  - **Information Warfare**
  - **Black Ops**
  - **Cyber Espionage**
  - Hacktivism
  - (private) **Cyber Armies**
  - Underground Economy and Black Markets
    - Organized Crime
    - Carders
    - Botnet owners
    - 0days
    - Malware factories (APTs, code writing outsourcing)
    - Lonely wolves
    - “cyber”-Mercenaries

Cybercrime MO



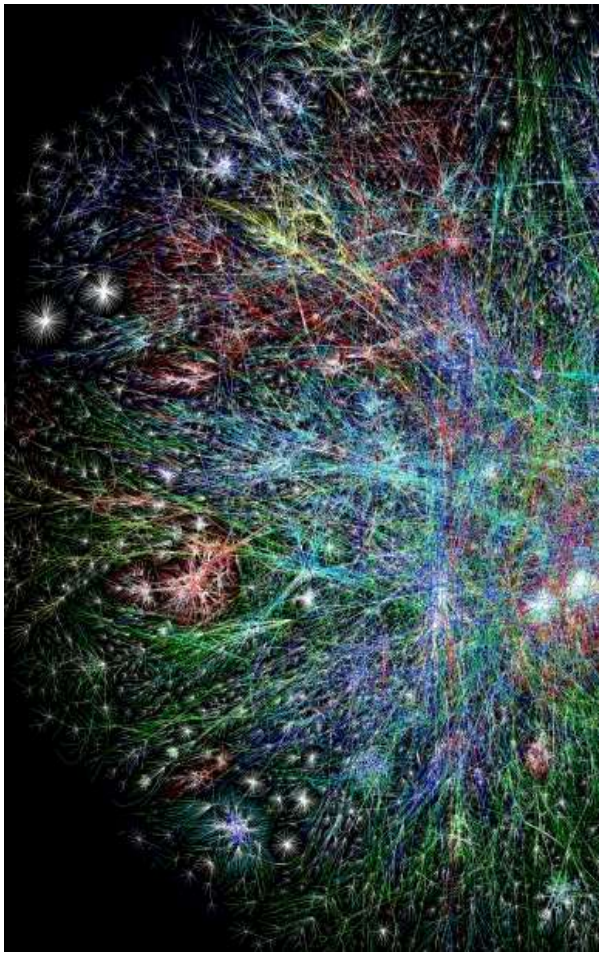
Profiling Actors

New Actors joined in

- **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

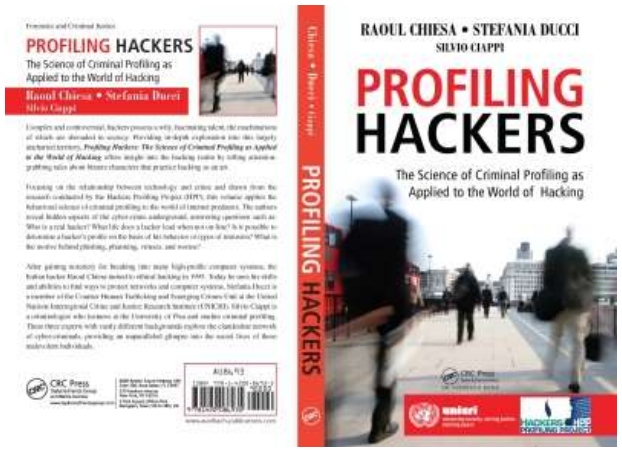
Everyone against everybody



Welcome to HPP!

HPP V1.0

- Back in **2004** we launched the Hacker's Profiling Project - HPP: http://www.unicri.it/special_topics/cyber_threats/
- Since that year:
  - **+1.200 questionnaires** collected & analyzed
  - **9 Hackers profiles** emerged
  - **Two books** (one in English)
    - Profilo Hacker, Apogeo, 2007
    - Profiling Hackers: the Science of Criminal Profiling as Applied to the World of Hacking, Taylor&Francis Group, CRC Press (2009)



unicri
advancing security, serving justice, building peace

Evaluation & Correlation standards

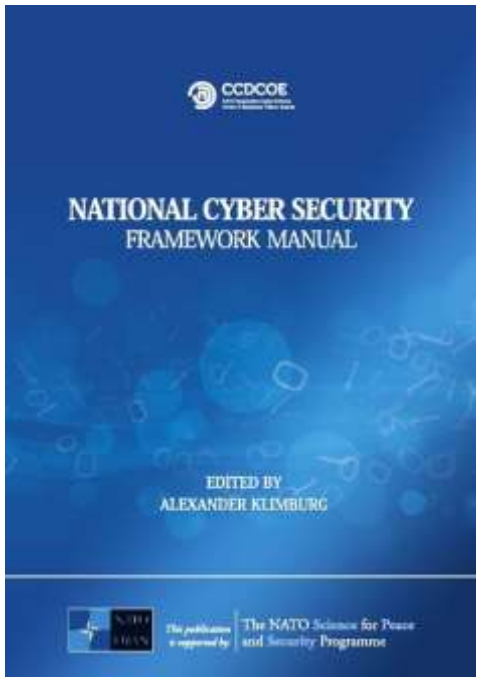
- Modus Operandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker's ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions and technical difficulties as a deterrent

unicri
advancing security, serving justice, building peace

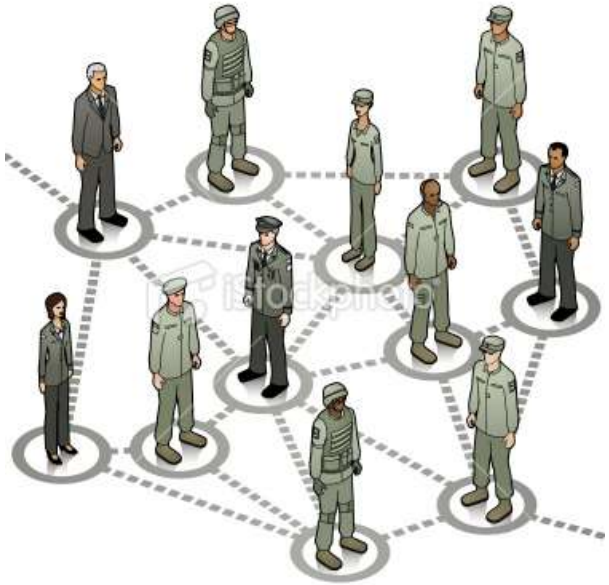
	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent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

Information Warfare (Cyberwar?)

(this section includes material from Prof. Dr. Alexander Klimburg)



The DUMA knew it, long time ago….



"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

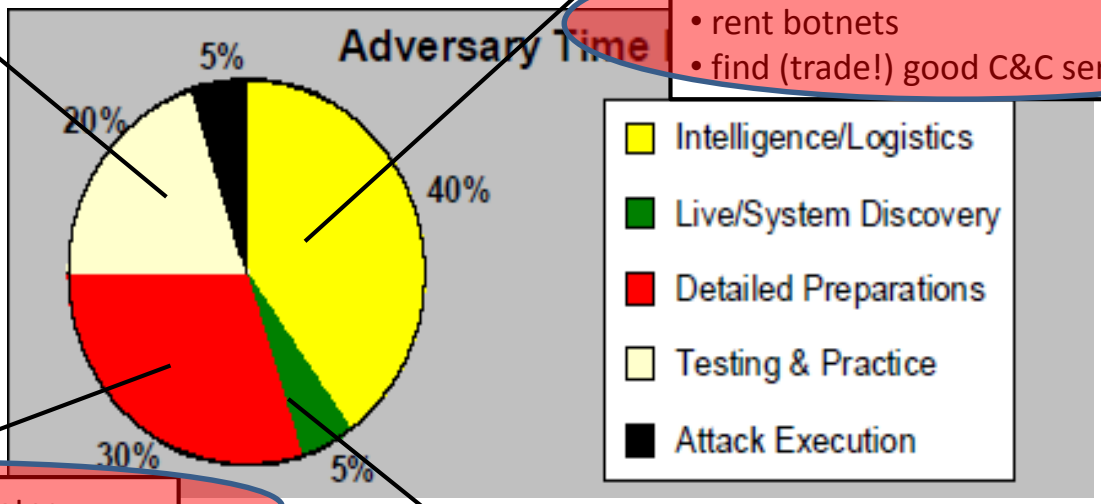
Cyber* Military Trends

OUT ☹	IN ☺
Single operational pic	Situational awareness
Autonomous ops	Self-synchronizing ops
Broadcast information push	Information pull
Individual	Collaboration
Stovepipes	Communities of Interest
Task, process, exploit, disseminate	Task, post, process, use
Multiple data calls, duplication	Only handle information once
Private data	Shared data
Perimeter, one-time security	Persistent, continuous IA
Bandwidth limitations	Bandwidth on demand
Circuit-based transport	IP-based transport
Single points of failure	Diverse routing
Separate infrastructures	Enterprise services
Customized, platform-centric IT	COTS based, net-centric capabilities
	Scouting elite hacker parties?

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

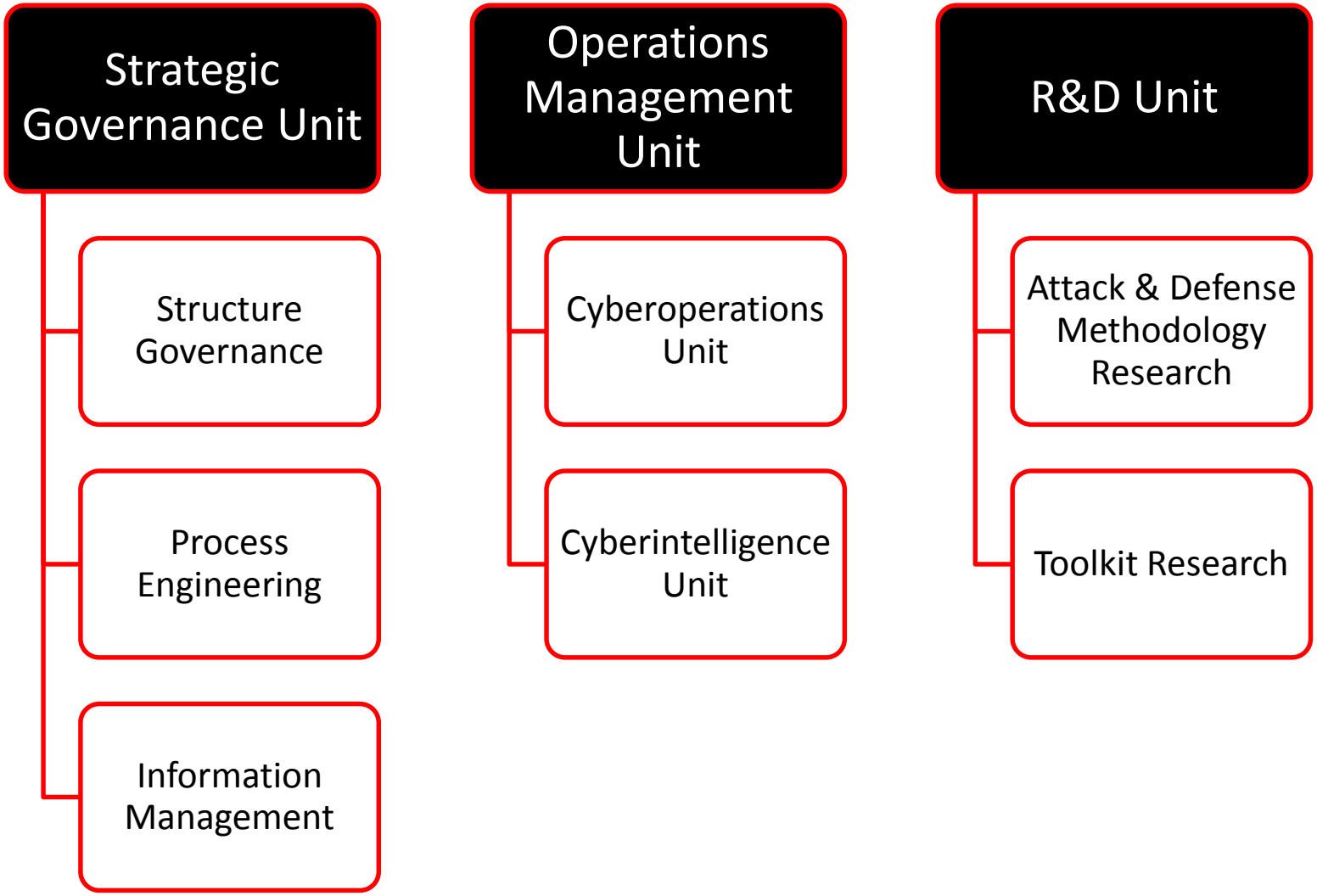


- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

•Purchase L2/L3 system data

Alexander Klimburg 2012

Possible CWUs Structure



Cyber Espionage: a case study from India

Cyber Espionage

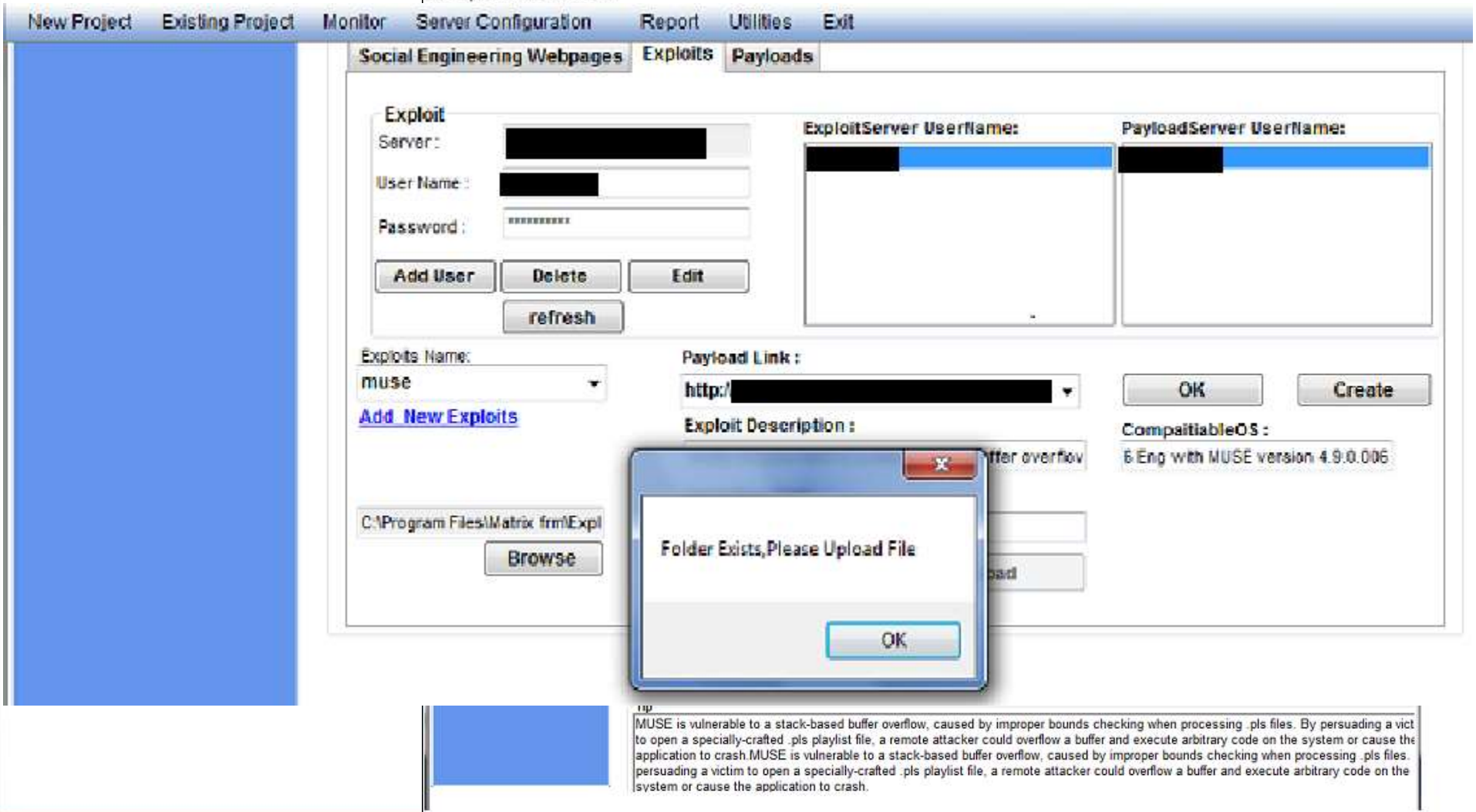
- The **complexity** and the **infrastructural and operating costs** of espionage (in the wide sense of the term) dramatically lowered down along the years, because of the IT revolution and the so-called "Digital Society".
- In most of the cases, the **information** sits on (also, or "just") on **digital storages** and **travels over the Net**.
- As a first effect, the **concept of "stealing" doesn't exist anymore** (it's virtual) and we must speak about **copying** the information (espionage approach):
  - What is "still there", is "safe";
  - More time needed to realize the "theft";
  - Less time needed to transfer or reselling the information -> cashing out.
- (public) incidents do happen both in the **private** and **public** (even **Military** and **Governmental**) business:
  - **insiders** (drivers: political, ethics, religious, fame and mass media, corruption, blackmail, ignorance);
  - **contractors** (external suppliers, consultants, VPN and RAS access, etc);
  - "**competitors**" (civilian and military) both *State-Sponsored* and *Independent.*

aMatrix Help

Exploits

Exploit Server Configuration

In Server Configuration of Exploit,you can create the exploit by choosing payload server userName,providing Exploit name,browse to choose .bin file and select payload link from the combobox and then click on OK and then Create button.After that choose Exploit server userName and providing Exploit description.You can also Create a folder on local machine as well as on server through FTP and upload File inside it.



Mistakes from MoDs, when dealing with these topics

Typical mistakes

- After having worked over the last five years with different MoDs from Europe, GCC and Asia-Pacific, I've been able to identify some issues…

1. Generational problem: Decision-makers are too old, often they don't speak English and they don't really know the topic. Younger Officials don't have the needed decision-power.
2. Terminology problems: «cibernetic» to us means something else… ☺
3. Lack of *internationally-agreed* laws on «cyber attacks» (UN, where are you?)
   - ITU Dubai 2012 showed this from another PoV (see later).
4. Not understanding of Information Security real-life: they relay on Vendors.
5. Mostly focus on preventive defense (and they do it wrong: lack of international information exchanges… «I wanna get, but I can't give out»…)
   - …while they would like to play with Offensive Operations.
6. Lack of know-how on hacking's history, mood, people - and underground conferences.
7. Not flexible procedures / environments – and mindsets: they spend MLNs for missiles and jet-fighters, while they argue on 0days prices (this happens all over).
8. Tough people, not so «flexible». But once you'll get intimate with them, they are just humans, as all of us.
9. Strict rules and procedures: doesn't allow them to «think out of the box».
10. It's so hard to explain them they need mixed, hybrid teams.
    - And, each country just want their own national experts into these teams.

«Attack attribution»

„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**

Source: Alexander Klimburg, 2012

Mistyping may lead to (very) different scenarios…

Non-state proxies and "inadvertent Cyberwar":

„ 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)***

Conclusions

Conclusions

- **Everything has changed**.
- You just **cannot fight on your own** this war anymore. You may win a single battle, while **it won't be enough**.
  - **If you are insecure, I will be insecure too**….
- Information Sharing, Security Awareness, Attacker's Profiling, balanced InfoSec approach & processes: **this is what you need**.
- Ask for technical solutions from the Security Industry, be compliant with security standards and regulations, but **don't forget both taking from and giving back to the security communities**.

References

[1] http://www.dsd.gov.au/infosec/csoc.htm

[2] Gary Waters, Desmond Ball, Ian Dudgeon, "Australia and cyber-warfare", Australian National University. Strategic and Defence Studies Centre, ANU E press, 2008

[3] http://www.dsd.gov.au/

[4] http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

[5] http://www.reuters.com/article/2012/03/08/china-usa-cyberwar-idUSL2E8E801420120308

[6] http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826

[7] http://www.atimes.com/atimes/China/NC15Ad01.html

[8] http://eng.mod.gov.cn/Opinion/2010-08/18/content_4185232.htm

[9] http://www.reuters.com/article/2011/06/01/us-korea-north-hackers-idUSTRE7501U420110601

[10] http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html

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

[12] Jeffrey Carr, "Inside Cyber Warfare: Mapping the Cyber Underworld", O'Reilly, December 2011

[13] http://www.nato.int/cps/en/SID-C986CC53-5E438D1A/natolive/topics_78170.htm?

[14] Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of means and motivations of selected Nation State", Darthmouth College, Dec. 2004

[15] http://www.defence.pk/forums/indian-defence/122982-new-war-between-india-pakistan-cyber-warfare.html

[16] http://www.dnaindia.com/india/report_as-cyber-attacks-rise-india-sets-up-central-command-to-fight-back_1543352-all

[34] http://www.jpost.com/Defense/Article.aspx?id=249864

[35] http://internet-haganah.com/harchives/006645.html

[36] http://articles.timesofindia.indiatimes.com/2010-10-16/india/28235934_1_cyber-security-hackers-official-agencies

[37] http://fmso.leavenworth.army.mil/documents/Russianvuiw.htm

[38] http://www.conflictstudies.org.uk/files/Russian_Cyber_Command.pdf

[39] http://www.defense.gov/news/newsarticle.aspx?id=65739

[40] http://www.defense.gov/news/newsarticle.aspx?id=65739

[41] http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf

[42] http://www.enisa.europa.eu/media/news-items/enisa-teams-up-with-member-states-on-pan-european-exercise

[43] http://english.nctb.nl/current_topics/Cyber_Security_Assessment_Netherlands/

[44] http://www.ccdcoe.org

Contacts, Q&A

- **Need** anything, 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?