



**SecurityBrokers**

GLOBAL CYBER DEFENSE & SECURITY SERVICES

**From Hacking to Cyber Warfare:  
the “fil rouge” among  
different Worlds, Ecosystems and Actors**

**Raoul Chiesa**

**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 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
  - New Actors & Ecosystems
- Conclusions
- References





# The Speaker

- **President, Founder, The Security Brokers**
- **Founder, Swascan.com**
- **Independent 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 @ European Union Network & Information Security Agency)*
- **Founder, @ CLUSIT** *(Italian Information Security Association)*
- **Steering Committee, AIP/OPSI** *(Privacy & Security Observatory)*
- **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 Attachè. Scientific Committee, APWG European Chapter**
- **Former Board Member, AIC** *(Italian Association of Critical Infrastructures)*
- **Supporter at some security community**



# 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, extortion)**
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, anonymity, 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)

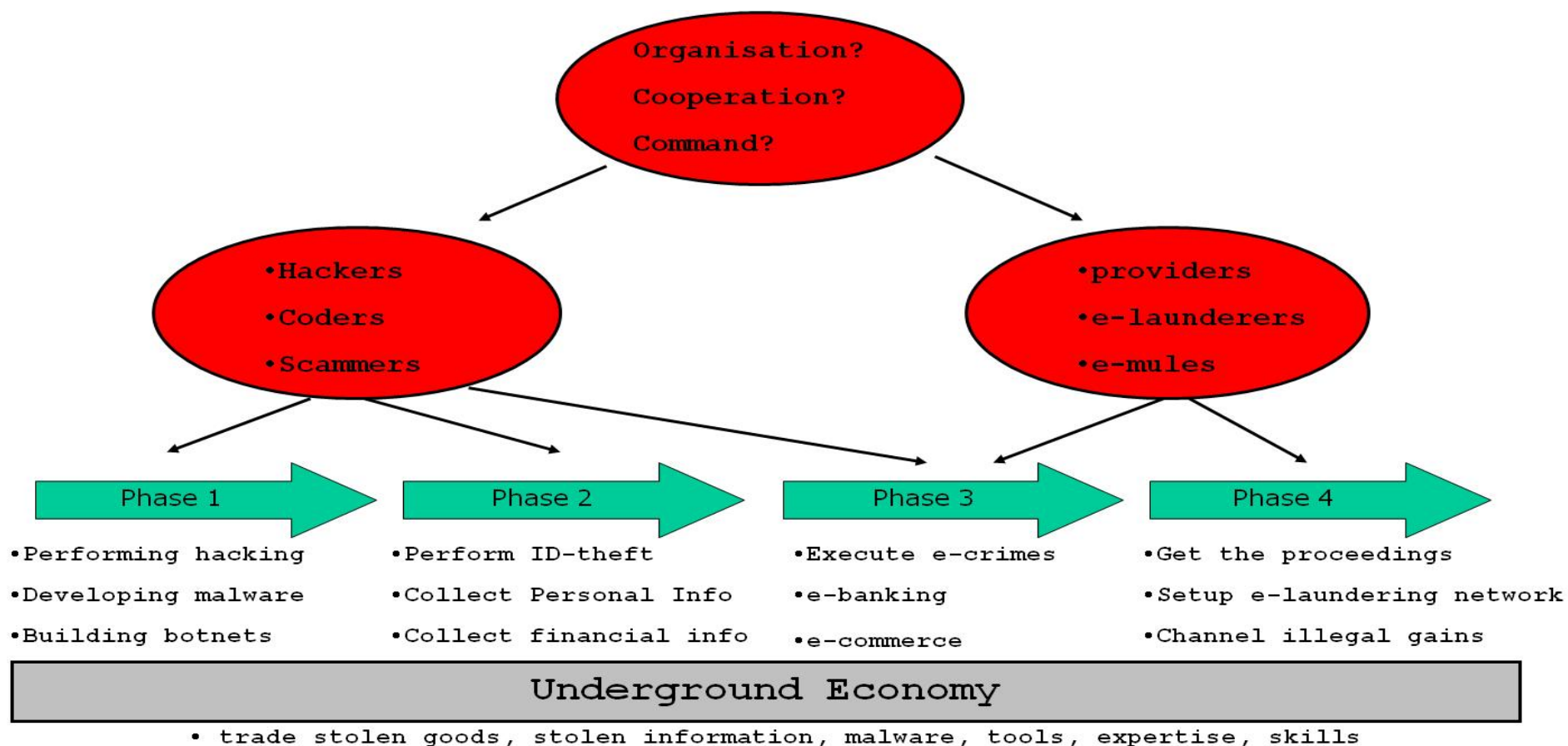
*2018 Financial Turnover, estimation:  
60B USD\$/year*



# 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
    - Odays
    - Malware factories (APTs, code writing outsourcing)
    - Lonely wolves
    - “cyber”-Mercenaries

# Cybercrime MO



# ***Profiling Actors***

# Welcome to HPP!



**unieri**

advancing security, serving justice,  
building peace



# HACKERS HPP PROFILING PROJECT



# HPP V1.0

\* Back in **2004** we launched the Hacker's Profiling Project - HPP:

[http://www.unicri.it/special\\_topics/cyber\\_threats/](http://www.unicri.it/special_topics/cyber_threats/)

\* Since that year:

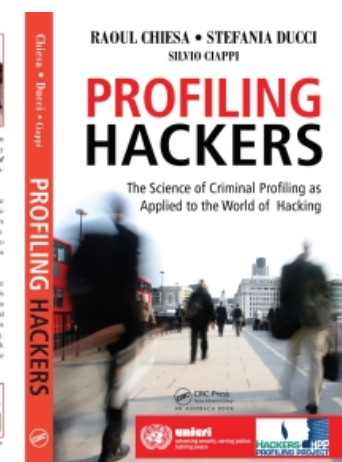
\* **+1.200 questionnaires** collected & analyzed

\* **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**

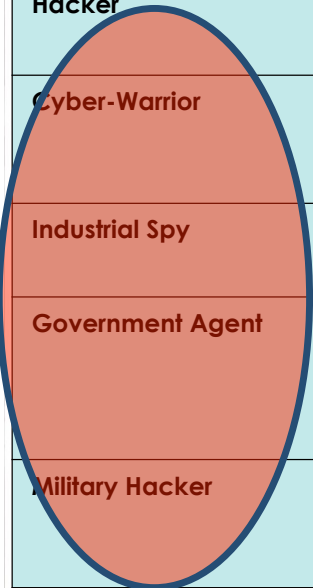


**unieri**

advancing security, serving justice,  
building peace



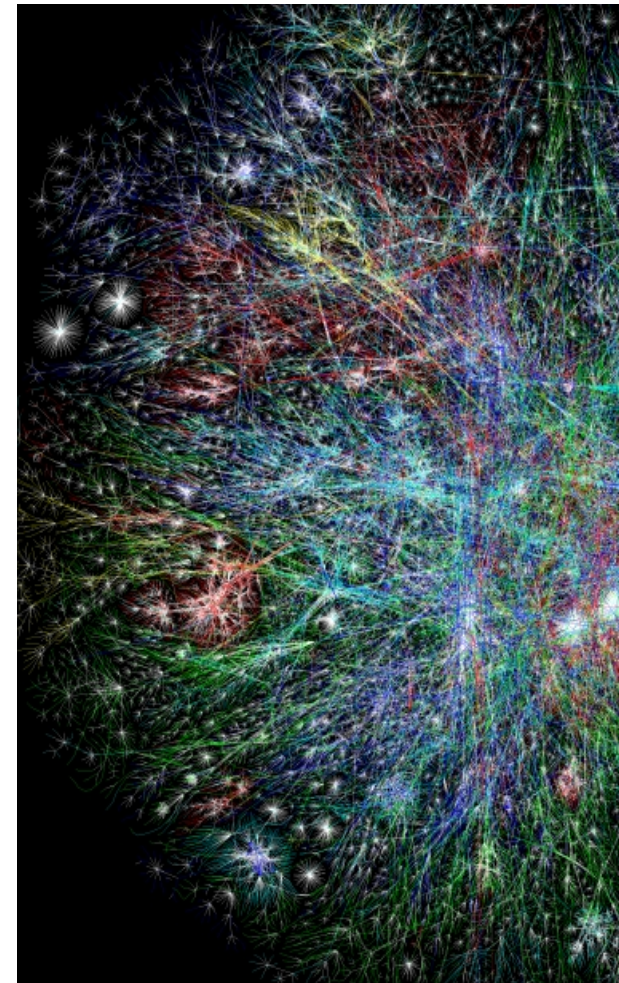
	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent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



# Then, new Actors joined in

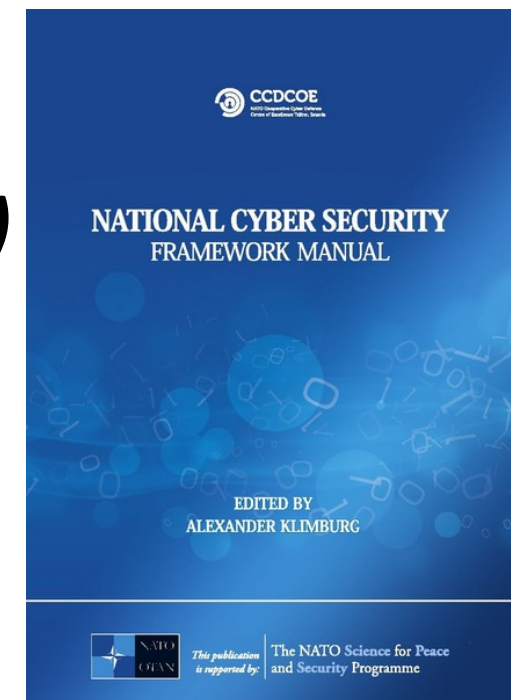
- \* **Cybercrime and Information Warfare** have a **very wide spectrum of action** and use **intrusion techniques** which are nowadays, somehow, available to a **growing amount of Actors**, which use them in order to **accomplish different goals**, with **approaches and intensity which may deeply vary**.
- \* **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**



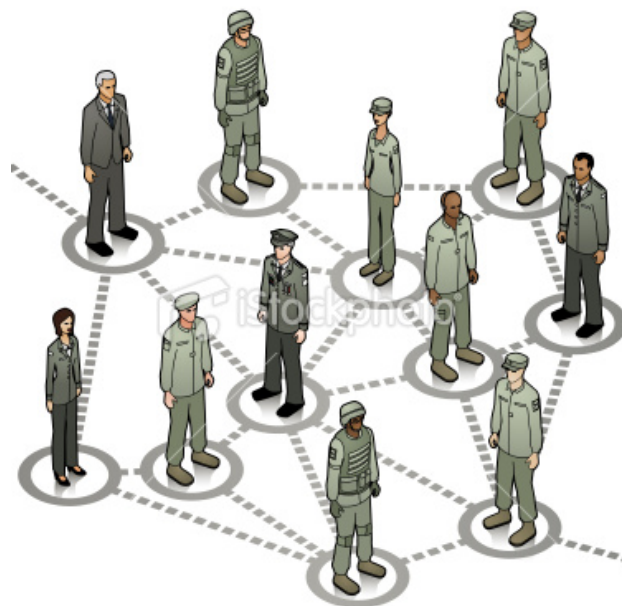
# ***Information Warfare (Cyberwar?)***

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





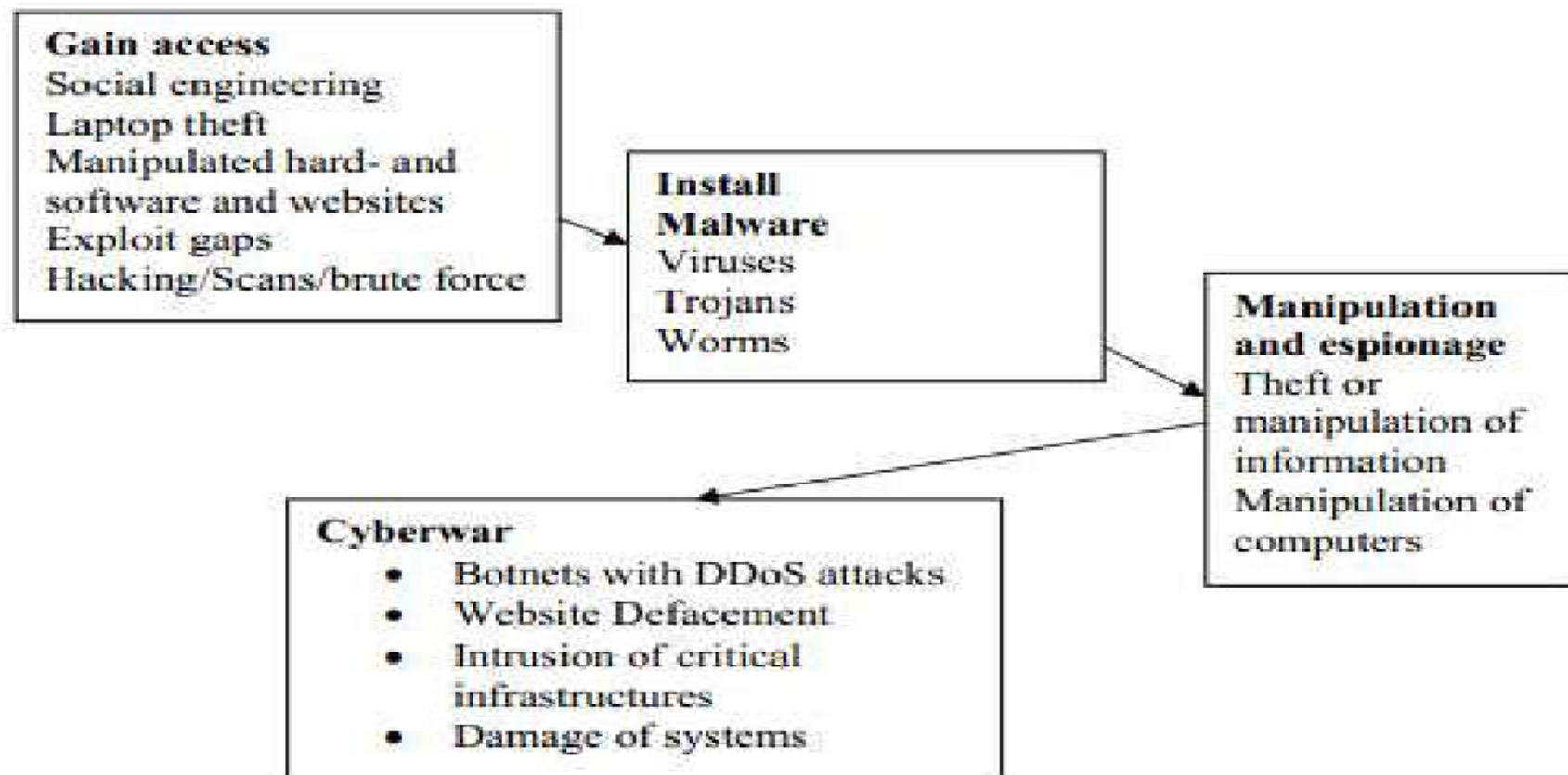
## The DUMA knew it, long time ago....



**"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**

...but, Saalbach knew this already in 2004!



Source: Saalbach: «Cyberwar Methods & Practice»

# Cyber\* Military Trends

**OUT ☹️**

Single operational pic  
Autonomous ops  
Broadcast information push  
Individual  
Stovepipes  
Task, process, exploit, disseminate  
Multiple data calls, duplication  
Private data  
Perimeter, one-time security  
Bandwidth limitations  
Circuit-based transport  
Single points of failure  
Separate infrastructures  
Customized, platform-centric IT

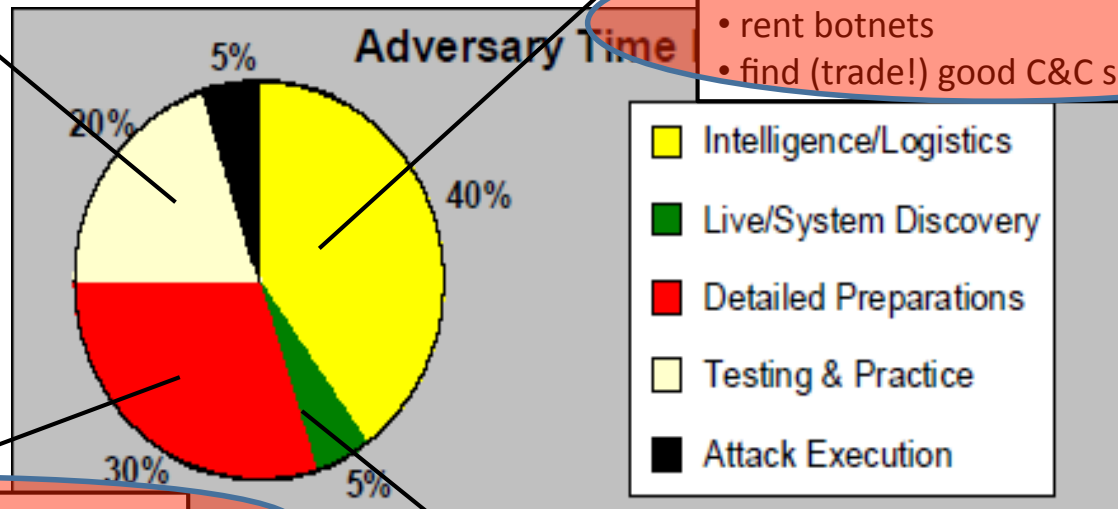
**IN 😊**

Situational awareness  
Self-synchronizing ops  
Information pull  
Collaboration  
Communities of Interest  
Task, post, process, use  
Only handle information once  
Shared data  
Persistent, continuous IA  
Bandwidth on demand  
IP-based transport  
Diverse routing  
Enterprise services  
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

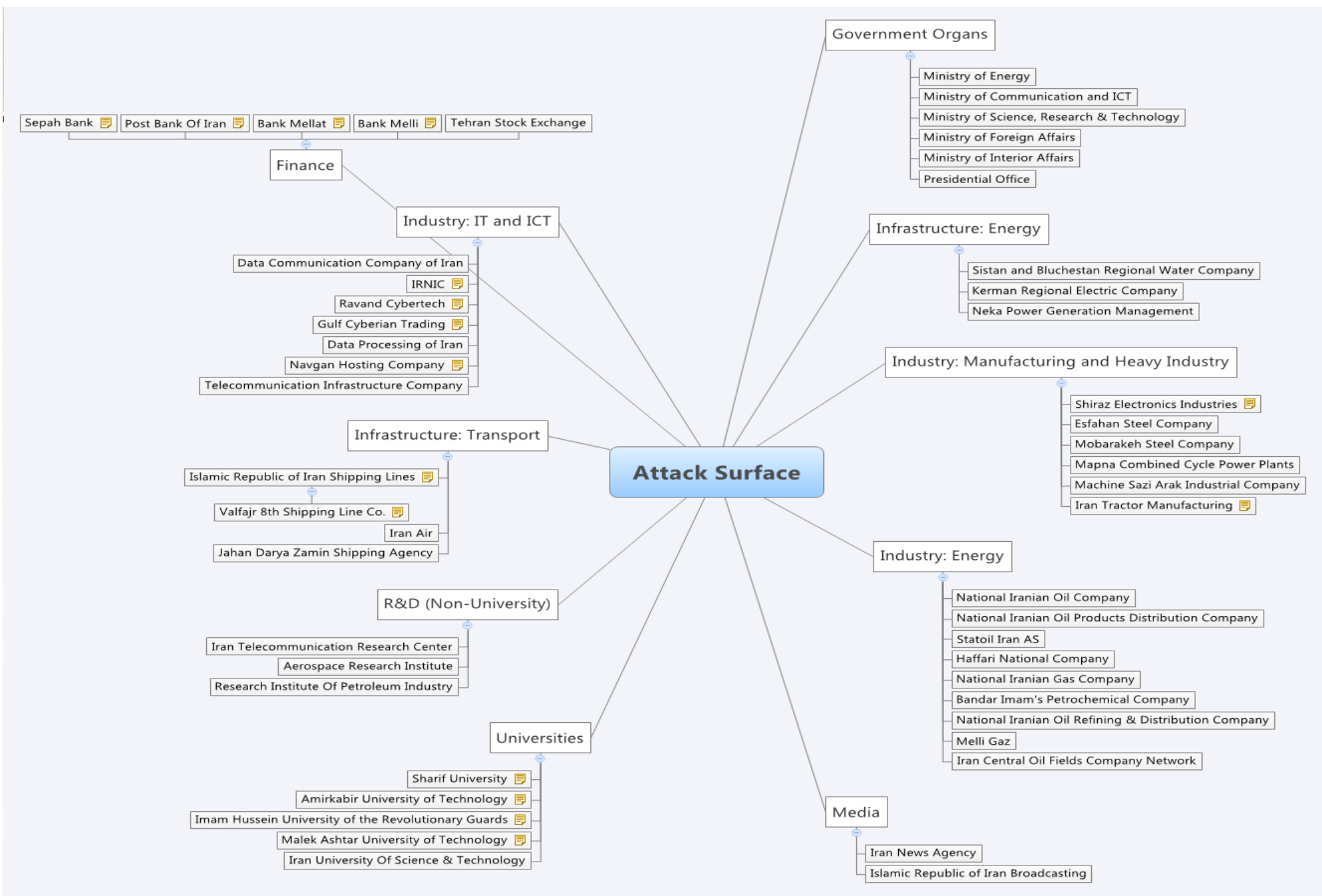


- Intelligence/Logistics
- Live/System Discovery
- Detailed Preparations
- Testing & Practice
- Attack Execution

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

- Purchase L2/L3 system data

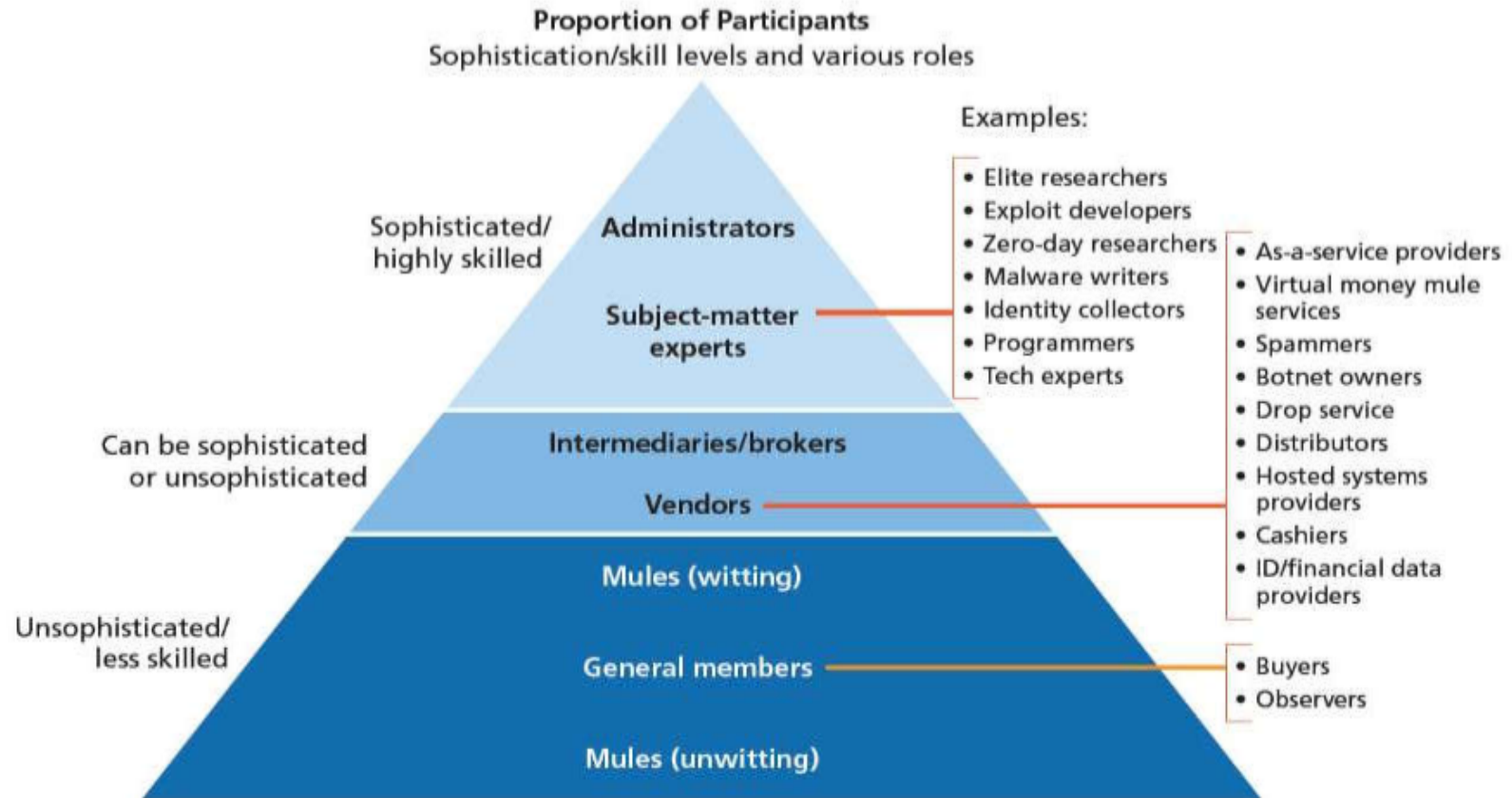
Alexander Klimburg 2012





# Mix of Actors generate new Ecosystems

Figure 2.1  
Different Levels of Participants in the Underground Market



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.  
NOTE: Almost any participant can be a ripper; see text for discussion.

RAND RR610-2.1

# The pricing debate



**Top Level Telecommunications**

[www.electrospaces.net](http://www.electrospaces.net)

May 6, 2014

**Pictures from inside the German intelligence agency BND**

(Updated: June 12, 2014)

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

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

The former Pullach headquarters

Welcome to this weblog about Top Level Telecommunications!

Here you can read about:

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

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

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

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

[http://www.theregister.co.uk/2014/11/11/german\\_spoops\\_want\\_millions\\_to\\_buy\\_0day\\_vulns/](http://www.theregister.co.uk/2014/11/11/german_spoops_want_millions_to_buy_0day_vulns/)

# The pricing debate

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

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

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

8

Adaptable System Recovery (ASR) for Linux virtual machines

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

### RELATED STORIES

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

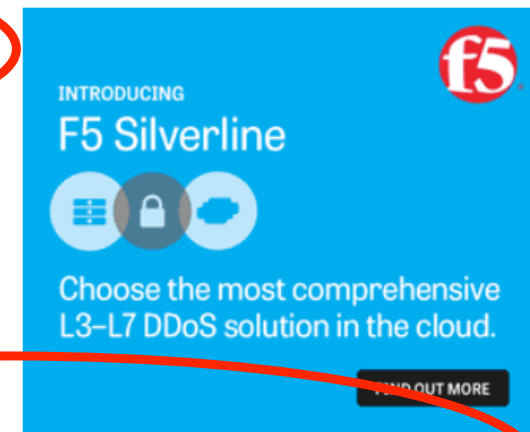
If you're suing the UK govt, Brit spies will snoop on your briefs

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

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

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

Kömer is also critical of the strategy on the basis that governments shouldn't be helping fund the grey market for security vulnerabilities, a sentiment echoed by the CCC



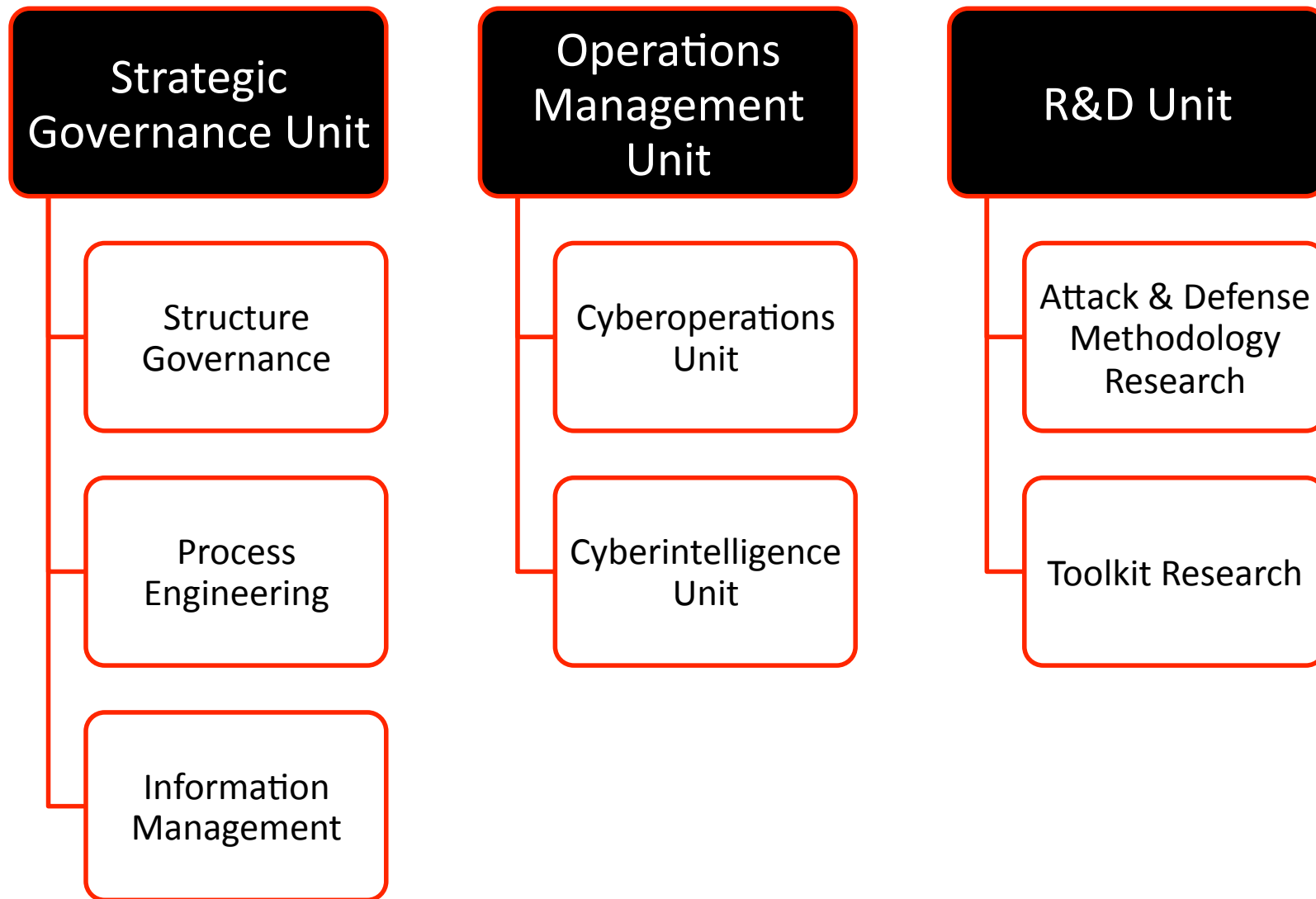
INTRODUCING  
F5 Silverline

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

[FIND OUT MORE](#)

[http://www.theregister.co.uk/2014/11/11/german\\_spooks\\_want\\_millions\\_to\\_buy\\_0day\\_vulns/](http://www.theregister.co.uk/2014/11/11/german_spooks_want_millions_to_buy_0day_vulns/)

# Possible CWUs Structure





# «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 8<sup>th</sup> 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”:

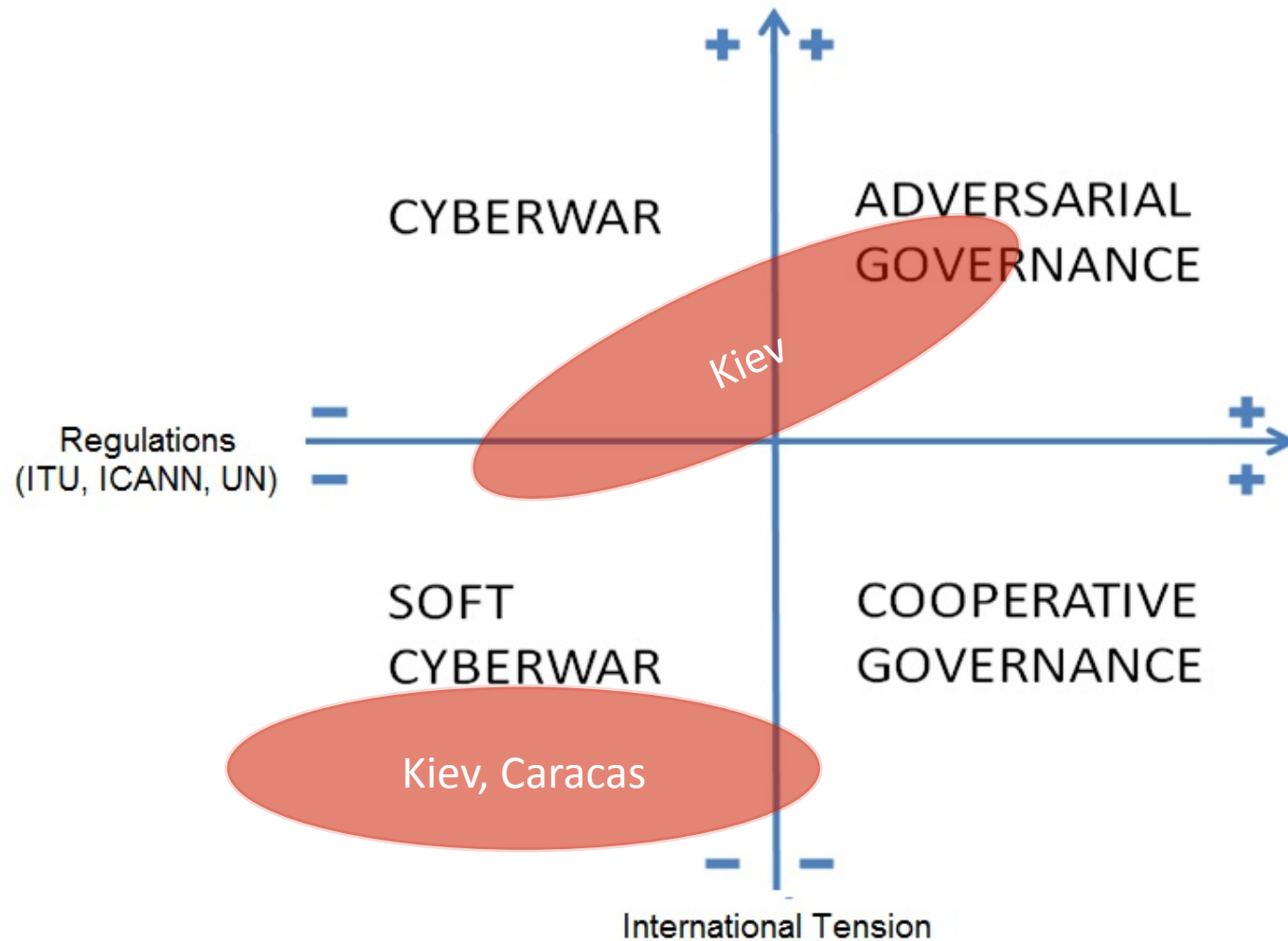
*„ During a time of international crisis, a [presumed non-state CNE] proxy network of country A is used to wage a „serious (malicious destruction) cyber-attack“ against country B.“*

**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**)*

© Alexander Klimburg 2012

# Evolving scenarios: 2014-2020



# *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](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/qIQAvWwloJ\\_story.html](http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/qIQAvWwloJ_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?](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", Dartmouth 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](http://www.dnaindia.com/india/report_as-cyber-attacks-rise-india-sets-up-central-command-to-fight-back_1543352-all)

34 <http://www.ipost.com/Defense/Article.aspx?id=249864>

35 <http://internet-haqanah.com/harchives/006645.html>

36 [http://articles.timesofindia.indiatimes.com/2010-10-16/india/28235934\\_1\\_cyber-security-hackers-official-agencies](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](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/NDAAs20Section2093420Report\\_For20webpage.pdf](http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAAs20Section2093420Report_For20webpage.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/](http://english.nctb.nl/current_topics/Cyber_Security_Assessment_Netherlands/)

44 <http://www.ccdcoe.org>



# Reading Room /1

**The commercialization of Digital Spying**, Morgan Marquis-Boire, Claudio Guarnieri, Bill Marczak, John Scott-Railton, Citizen Lab, Canada Center for Global Security Studies, Munk School of Global Affairs (University of Toronto), 2013

**No Place to Hide: Edward Snowden, the NSA and Surveillance State**, Glenn Greenwald, Penguin Books, 2014

**Grazie Mr. Snowden**, Fabio Chiussi, edizioni ValigiaBlu/Messaggero Veneto, 2014

**Kingpin**, Kevin Poulsen, 2012

**Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking**, Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009

**H.P.P. Questionnaires 2005-2010**

**Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet**, Joseph Menn, Public Affairs, 2010

**Stealing the Network: How to Own a Continent, (an Identity), (a Shadow)** (V.A.), Syngress Publishing, 2004, 2006, 2007

**Stealing the Network: How to Own the Box**, (V.A.), Syngress Publishing, 2003

**Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier**, Suelette Dreyfus, Random House Australia, 1997

**The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, Clifford Stoll, DoubleDay (1989), Pocket (2000)

**Masters of Deception: the Gang that Ruled Cyberspace**, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

**Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997

**Takedown**, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

**The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997

**The Art of Deception**, Kevin D. Mitnick & William L. Simon, Wiley, 2002

**The Art of Intrusion**, Kevin D. Mitnick & William L. Simon, Wiley, 2004

**@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998

# Reading Room /2

**The Estonia attack: Battling Botnets and online Mobs**, Gadi Evron, 2008 (white paper)

**Who is “n3td3v”?**, by Hacker Factor Solutions, 2006 (white paper)

**Mafiaboy: How I cracked the Internet and Why it's still broken**, Michael Calce with Craig Silverman, 2008

**The Hacker Diaries: Confessions of Teenage Hackers**, Dan Verton, McGraw-Hill Osborne Media, 2002

**Cyberpunk: Outlaws and Hackers on the Computer Frontier**, Katie Hafner, Simon & Schuster, 1995

**Cyber Adversary Characterization: auditing the hacker mind**, Tom Parker, Syngress, 2004

**Inside the SPAM Cartel: trade secrets from the Dark Side**, by Spammer X, Syngress, 2004

**Hacker Cracker**, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

**Compendio di criminologia**, Ponti G., Raffaello Cortina, 1991

**Criminalità da computer**, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

**United Nations Manual on the Prevention and Control of Computer-related Crime**, in International Review of Criminal Policy – Nos. 43 and 44

**Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale**, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

**Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques**, Turvey B., Knowledge Solutions Library, January, 1998

**Malicious Hackers: a framework for Analysis and Case Study**, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

**Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro

# Contacts, Q&A

\* **Need** anything, got **doubts**, wanna ask me smth?

\* rc [at] security-brokers [dot] com

**Thanks for your attention!**

**QUESTIONS?**

