Information Warfare.

Mistakes from the MoDs.

Raoul «Nobody» Chiesa

Founder, Partner, **Security Brokers**

Principal, **CyberDefcon Ltd**.

Partner, **T**elecom **S**ecurity **T**ask **F**orce

SecurityBrokers
Global Cybersecurity Defense Services

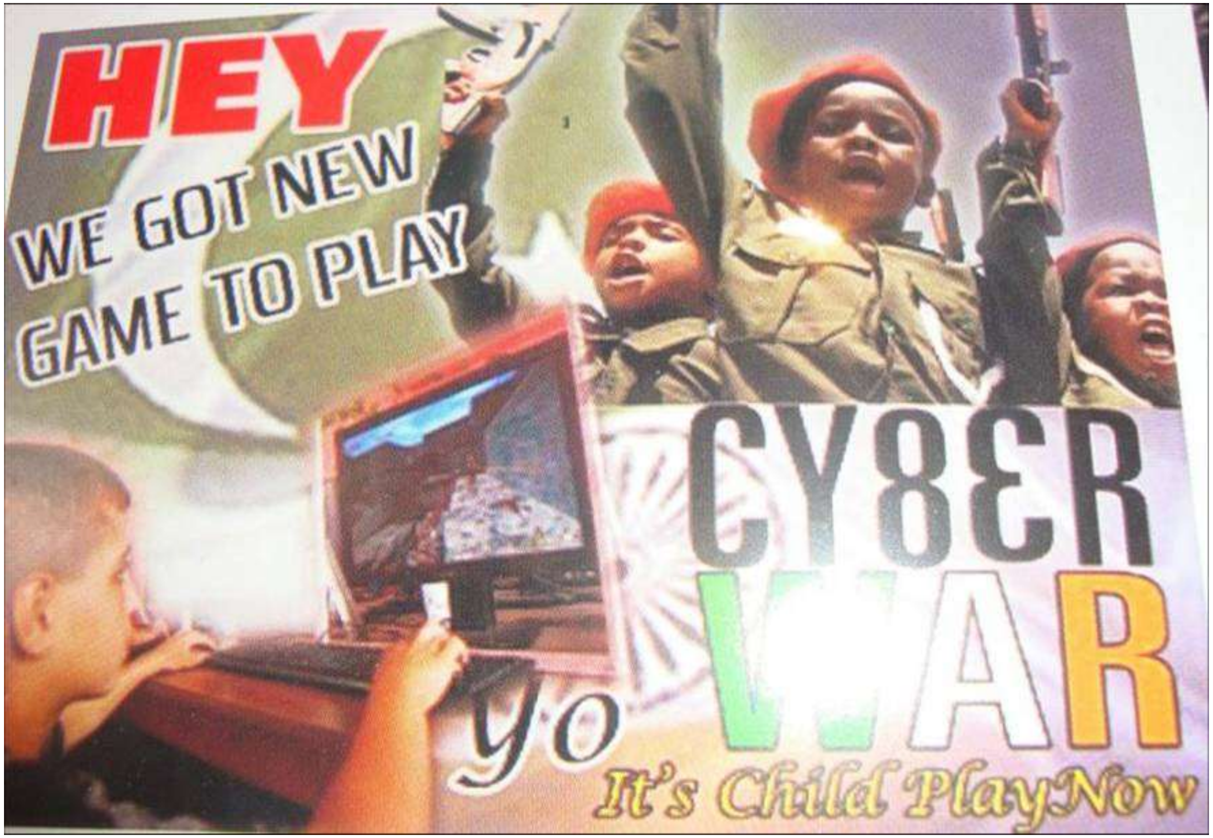
TSTF.net
Telecom Security Task Force

CyberDefcon

Keynote, Day 3 – May 4th, 2013

This is the Agenda

- Disclaimer
- Introductions
- Scenarios
- Nation's worldwide status
- Problems
- Conclusions
- Contacts, Q&A



Disclaimer

→Disclaimer

The views expressed are those of the author(s) and speaker and **do not necessary reflect** the views of UNICRI, ENISA and its PSG, ISECOM, OWASP, Italian MoD and its WG “Cyber World” at CASD/OSN, nor the private companies and those security communities I’m working at and/or supporting.

Thanks and....**enjoy this final Key Note** ☺

Introductions

→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 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, Manager of the WG «Cyber World» @ **Italian MoD**

Board of Directors, **ISECOM**

Board of Directors, **OWASP** Italian Chapter

Supporter at various security communities

In a nutshell…

- This Key Note will (try to) analyze those mistakes commonly done by MoD while dealing with the so-called "Cyberwar".

- I will pass through cultural, practical, logistics and narrow-minds issues I’ve been able to observe while training various military staff in different countries.

Scenarios

→Learning from the past…

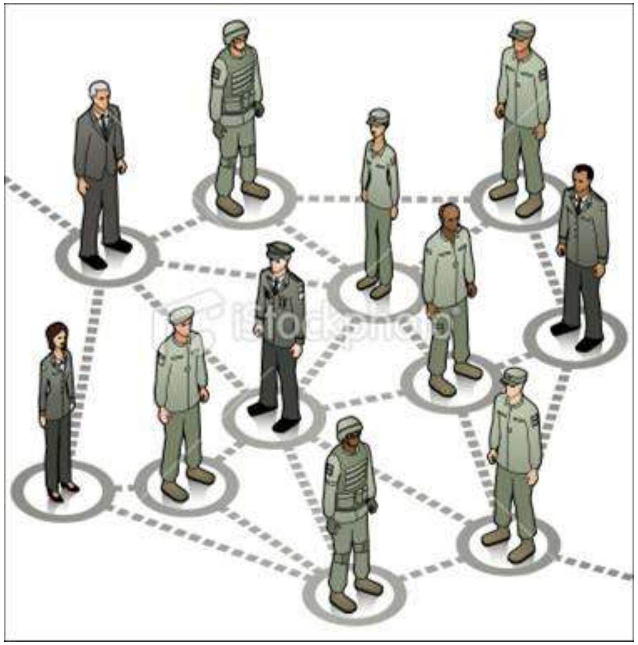
". . . attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence."

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

→ Back in 2007, a brilliant made sade something which was undevaluated



"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)

→ What happened 'till now?

2010: Report on Stuxnet Virus

2007: Aurora Experiment

1999: Moonlight Maze

2007: DDoS Attack against Estonia

2003: Cyber Attack Titan Rain

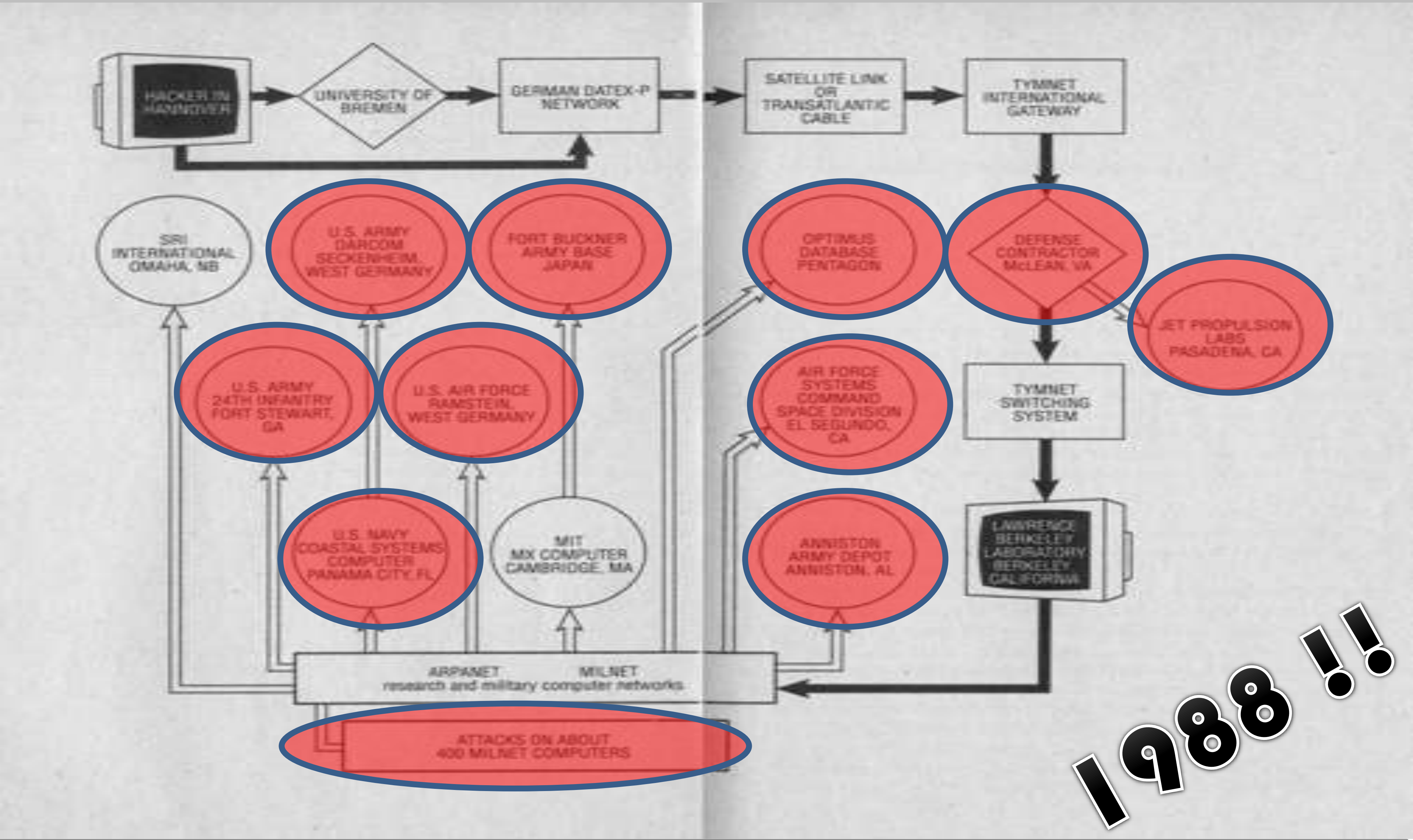
2010: Operation Payback

Source: Andrea Zapparoli Manzoni, Security Brokers

→ Right? NO!!!

Ehy, we're missing one important piece here (at least!)

→ Back to the 80's...


HACKER IN HANNOVER
UNIVERSITY OF BREMEN
GERMAN DATEX-P NETWORK
SATELLITE LINK OR TRANSATLANTIC CABLE
TYMNET INTERNATIONAL GATEWAY
SRI INTERNATIONAL OMAHA, NB
U.S. ARMY DARCOM SECKENHEIM, WEST GERMANY
FORT BUCKNER ARMY BASE JAPAN
OPTIMUS DATABASE PENTAGON
DEFENSE CONTRACTOR McLEAN, VA
JET PROPULSION LABS PASADENA, CA
U.S. ARMY 24TH INFANTRY FORT STEWART, GA
U.S. AIR FORCE RAMSTEIN, WEST GERMANY
AIR FORCE SYSTEMS COMMAND SPACE DIVISION EL SEGUNDO, CA
TYMNET SWITCHING SYSTEM
U.S. NAVY COASTAL SYSTEMS COMPUTER PANAMA CITY, FL
MIT MX COMPUTER CAMBRIDGE, MA
ANNISTON ARMY DEPOT ANNISTON, AL
LAWRENCE BERKELEY LABORATORY BERKELEY CALIFORNIA
ARPANET MILNET research and military computer networks
ATTACKS ON ABOUT 400 MILNET COMPUTERS

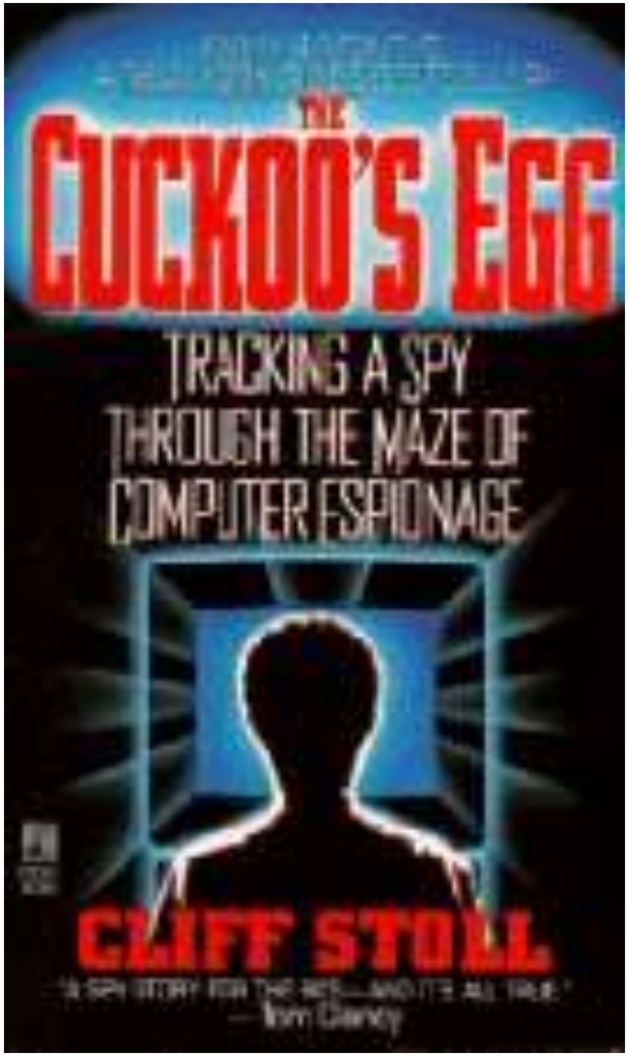
1988 !!

→ Back to the 80's...

- ❑ The **first worldwide-known** case about Soviet Union (KGB) hacking into US **defense contractors** and **critical Military and Government** infrastructures, using CCC.de's hackers:
  - ✓ 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, Forth Stewart, GA
  - ✓ SRI International, Omaha, NB
  - ✓ U.S. ARMY Darcom Seckenheim, **West Germany**

- ❑ 1989: **The Cuckoo's egg** by Clifford Stoll
  - http://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787/ref=pd_bbs_1/002-5819088-5420859?ie=UTF8&s=books&qid=1182431235&sr=8-1

→ Back to the 80's…Wanna learn more?


THE
CUCKOO'S EGG
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
CLIFF STOLL
"A SPY STORY FOR THE 90'S—AND IT'S ALL TRUE"
—Tom Clancy

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! :)

- ❑ **Intelligence Elements**
  - ✓ Information / Data
  - ✓ Subjects / Actors (Persons, Agents, Organizations)
  - ✓ Correlation, Analysis and Reporting

- ❑ **Intelligence Actions**
  - ✓ Protect
  - ✓ Obtain
  - ✓ Improve
  - ✓ Influence
  - ✓ Disturb
  - ✓ Destroy

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

- ❑ **Some good starters, here:**
  - ✓ http://en.wikipedia.org/wiki/Computer_network_operations
  - ✓ http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

- ❑ **IO = Information Operations**
  - ✓ US dominates this…
  - ✓ Lot of misunderstanding and false interpretations
  - ✓ A (very very) LOOOOONG list of terms… (I'm sorry for this! ☹

→ IO / Information Operations: Definitions /1

- 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 /2

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

→ IO / Information Operations: Definitions /3

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 /4

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
- SIGSEC = Signals

C-SIGINT = Counter-Signals Intelligence

ECM = Electronic Countermeasures

EMI = Electromagnetic Interference

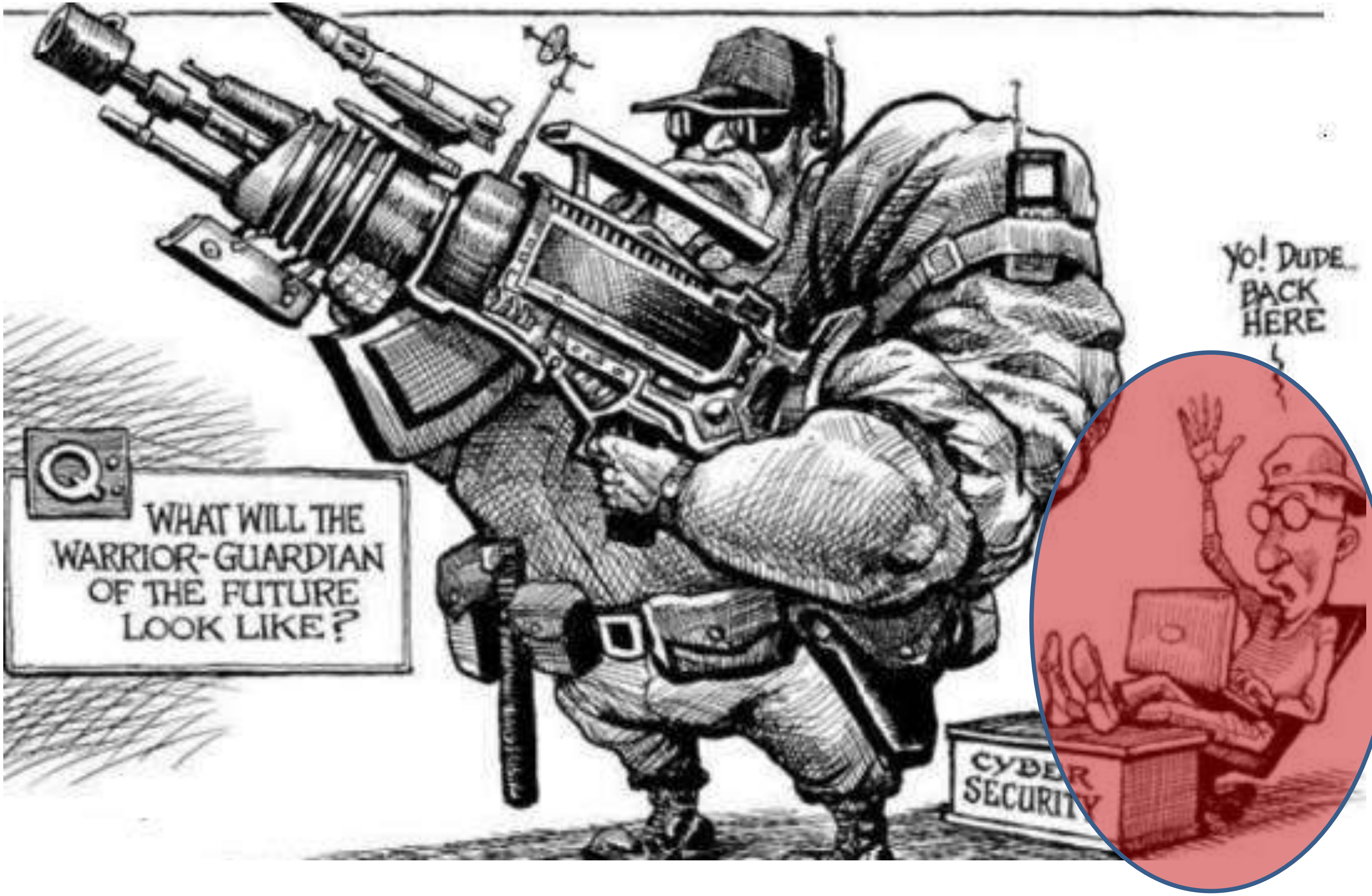
IBW = Intelligence-based Warfare

IEW = Intelligence and Electronic Warfare

(Additions welcome, mailto:indianz(a)indianz.ch)

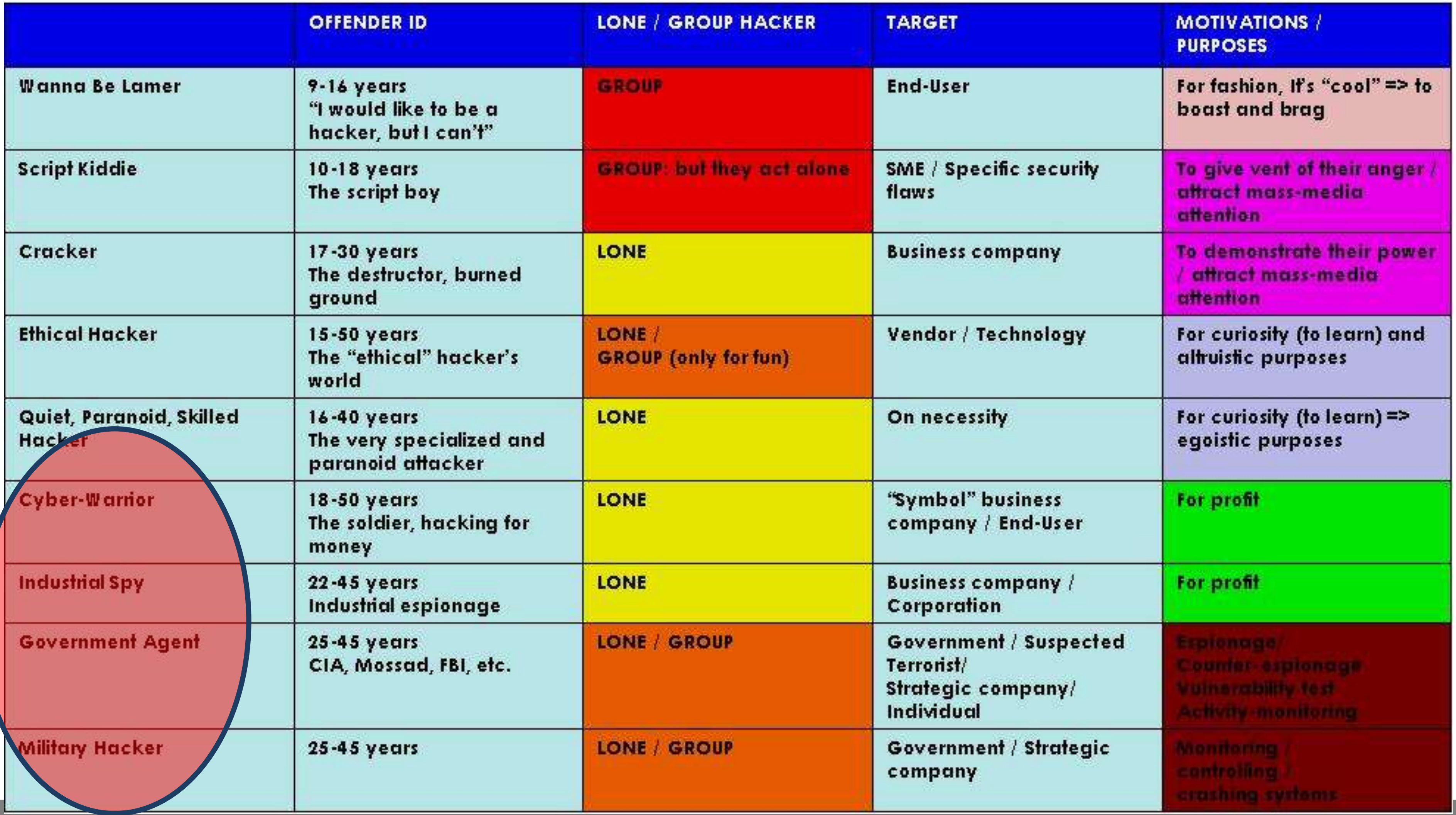
→ In real life: WHO is doing WHAT

- Is the actual scenario a real threat to National Security?
  - Exponential growth of ICT attacks
  - New actors join in:
    - Hacktivism world
    - Company to Company
    - Cyberwarriors (“outsourcing”)
    - Organized crime (Cybercrime + tools development)
- Rather, is it much more of an opportunity?
  - Moving from “old-school” war scenarios (and weapons)
  - Higher “cyber”-budgets
  - New companies
  - New players
  - Emerging countries (low entry-fee into the new world-chess)
- Cyber-attack in order to:
  - Industrial Espionage
  - Information manipulation
  - Supporting real-life operations
  - Cyber-warfare and cyber-weapons


Q
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE. BACK HERE
CYBER SECURITY

→ Profiling «Hackers» (United Nations, UNICRI, HPP V1.0 – 2004-2012)

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

→ Profiling «Hackers» (United Nations, UNICRI, HPP V2.0 – 2013-2015)

1. Wannabe Lamer
2. Script kiddie: under development (Web Defacers, DDoS, links with distributed teams i.e. Anonymous….)
3. Cracker: under development (Hacking on-demand, “outsourced”; links with Organized Crime)
4. Ethical hacker: under development (security researchers, ethical hacking groups)
5. Quiet, paranoid, skilled hacker (*elite*, unexplained hacks?)
6. Cyber-warrior: to be developed
7. Industrial spy: to be developed (links with Organized Crimes & Governments i.e. “The Comodo and DigiNotar” hacks?)
8. Government agent: to be developed (“N” countries..)
9. Military hacker: to be developed (India, China, N./S. Korea, etc.)

X. Money Mules? Ignorant “DDoSsers”? (i.e. LOIC by Anonymous)

→ Profiling «Hackers» (United Nations, UNICRI, HPP V2.0 – 2011-2012)

Going after Cybercriminals:

- **Kingpins & Master minds** (the “Man at the Top”)
  - Organized Crime
  - MO, Business Model, Kingpins – “How To”
    - i.e.: http://blog.eset.com/2011/10/18/tdl4-rebooted

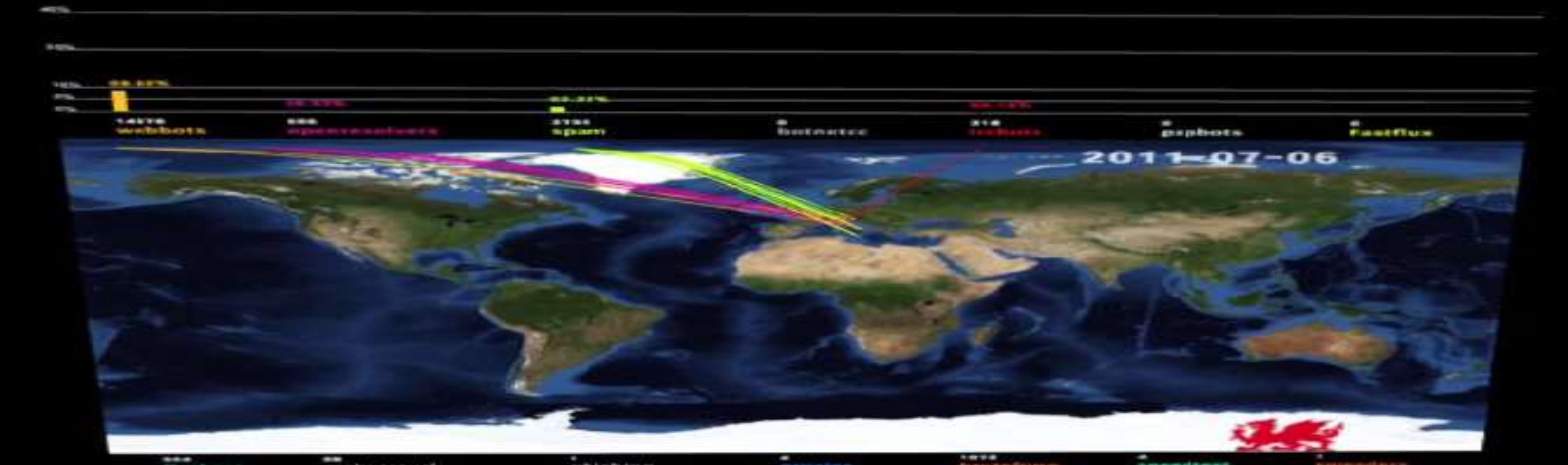
- **Techies hired by the Organized Crime** (i.e. Romania & skimming at the very beginning; Nigerian cons; Ukraine Rogue AV; Pharma ADV Campaigns; ESTDomains in Estonia; etc..)

- **Techies hired by the GOVs, MILs & INTs** (Vodafone Greece 2004, anyone remembers Freelancers? Old-school guys or retired engineers?)

- **Structure, Infrastructures** (links with Govs & Mils?)

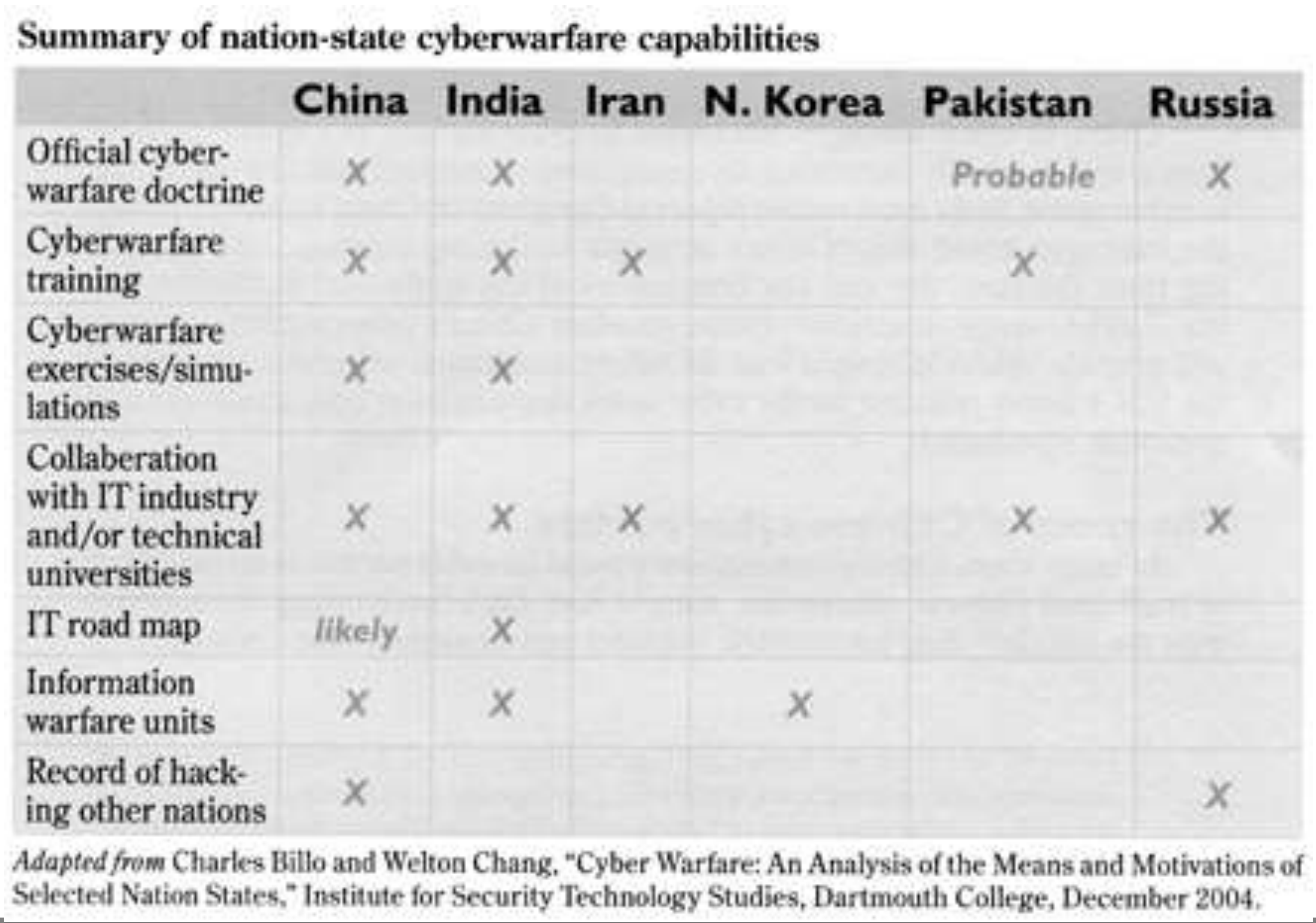
- **Money Laundering: Follow the money** (E-mules & new ways to “cash-out”)

- **Outsourcing: malware factories** (Stuxnet? DuQu??)



Nations Wordwide Status

→ I found this in 2004…



Summary of nation-state cyberwarfare capabilities

	China	India	Iran	N. Korea	Pakistan	Russia
Official cyberwarfare doctrine	X	X			*Probable*	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simulations	X	X				
Collaberation with IT industry and/or technical universities	X	X	X		X	X
IT road map	*likely*	X				
Information warfare units	X	X		X		
Record of hacking other nations	X					X

Adapted from Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States," Institute for Security Technology Studies, Dartmouth College, December 2004.

In a nutshell:– 2010 (Survey from Jart Armin & Raoul Chiesa – Cyberdefcon Ltd.)

Countries

- Russia
- USA
- France
- Israel
- UK
- China
- India
- Pakistan
- Ukraine
- Intl. Malware Factories

Activities

- Cyber crime tools
- Communications Intelligence
- National defence know-how
- Transition from Industrial tools
- Hired Cyber mercenaries
- Industrial espionage
- Counter cyber attacks
- Cyber army
- Botnet armies
- Contract developers (x 4 worldwide)

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

Nations with Cyber Warfare (Offensive) Capabilities

	Cyber warfare Doctrine/Strategy		CW training/ Trained Units	CW exercises/ simulations	Collaboration w/ IT Industry and/or Technical Universities	Not official Sources
Australia[,,]		X	X			
Belarus	X		X			
China[21]	X		X	X	X	,
North Korea[21]			X		X	,,
France[21,29]	X		X	X	X	
India[21, 31]	X		X	X	X	33
Iran[21,,,]			X		X	34, 35
Israel[21,]	X		X	X	X	
Pakistan[21,,]			X			36
Russia[21]	X		X		X	37, 38
USA[21, 30, 39 40,41]		X	X	X		

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

Nations with Cyber Defense Capabilities / 1

	Cyber warfare Doctrine/Strategy		CW training/ Trained Units	CW exercises/ simulations	Collaboration w/ IT Industry and/or Technical Universities
Albania[21,30]		X	X	X	
Argentina[21]	X		X		
Austria[21,24]	X		X	X	
Brazil[21]		X	X	X	
Bulgaria[21]		X		X	
Canada [5,30]				X	
Cyprus[21,42]		X	X	X	X
South Korea [21]		X			
Denmark[21,30]		X		X	
Estonia[21,30]		X	X	X	
Philippines[21]		X	X		X
Finland[12]	X			X	
Ghana[21]		X			
Germany[21,30]	X		X	X	
Japan[21]			X		
Jordan[21]		X	X		

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

Nations with Cyber Defense Capabilities / 2

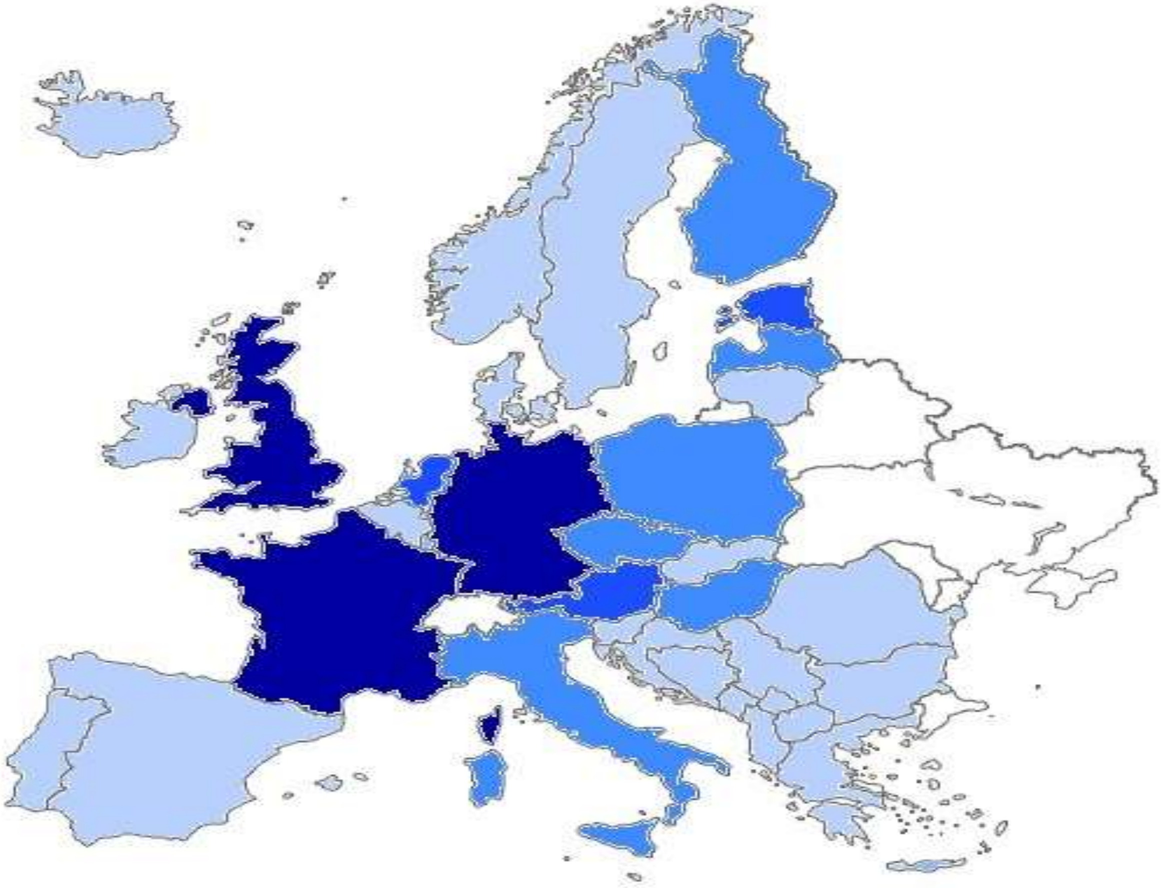
Italy[21,30]			X	X	X
Kenya[21]			X		
Latvia[21]		X	X	X	
Lithuania[21]		X		X	
Malaysia[21]		X	X		
New Zealand[21]		X	X		
Norway[21,30]		X		X	
Netherlands[21,8,43]		X	X	X	
Poland[21,30]		X		X	
Czek Republic[21,8]		X	X	X	
Slovak Republic[21,8]		X		X	
Spain[8]				X	
Sweden[21,,42]				X	
Switzerland[21,42]		X		X	
Turkey[21,29]		X	X	X	
Hungary[21]		X	X	X	X
United Kingdom[21,8]		X	X	X	

→ Key problems

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

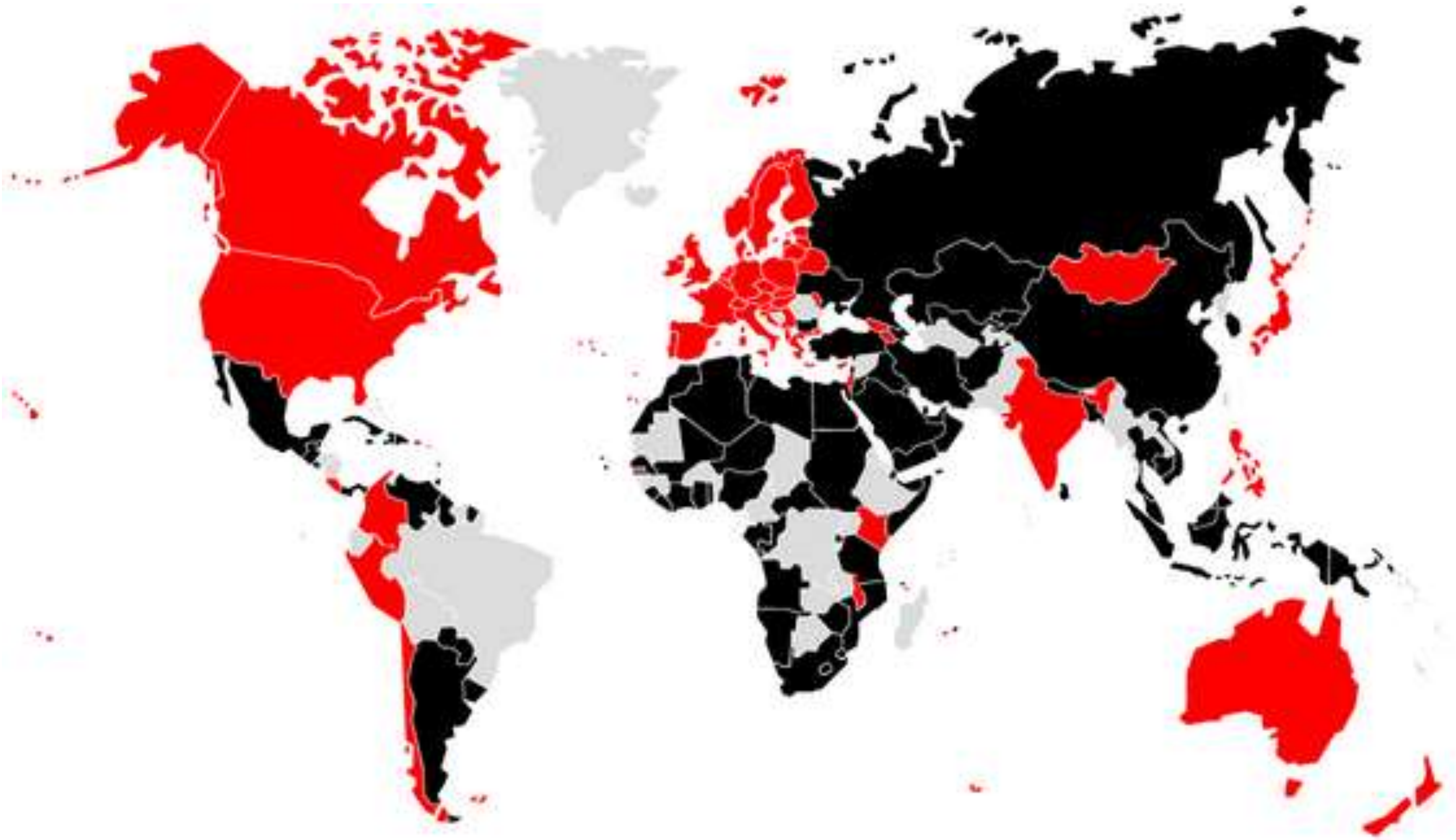
- ✓ **Generational problem**: Generals are too old, don't speak English and don't know the topic. Younger officials don't have the needed decision-power.
- ✓ **Terminology** problems: «cibernetic» to us means something else… ☺
- ✓ Lack of *internationally-agreed* **laws** on «cyber attacks» (**UN, where are you?**)
  - ✓ ITU Dubai 2012 showed this from another PoV (see later).
- ✓ **Not understanding** of Information Security real-life: they relay on **Vendors**.
- ✓ 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**.
- ✓ **Lack of** know-how on hacking's history, mood, people - and conferences.
- ✓ **Not flexible** procedures / environments – and mindsets: they spend MLNs for missiles, while they argue on 0days prices (this happens all over).
- ✓ **Tough people**. But once you'll get intimate with them, they are just humans, as all of us.
- ✓ **Strict rules and procedures**: doesn't allow them to «think out of the box».
- ✓ It's so hard to explain them they need **mixed, hybrid teams**.
  - ✓ And, each country just want **their own national experts** into these teams.

→ 2013 - Map of Cyber Defense evolving Member States (partial)



Source: Flavia Zappa, Security Brokers, 2013

→ 2013 - Map of ITU Dubai General Assembly December (red=not signed; black=signed)



Source: Flavia Zappa,
Security Brokers, 2013

→ The right words

- "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, **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.

→ 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

→ **Mistyping may lead to different scenarios…**

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**)*

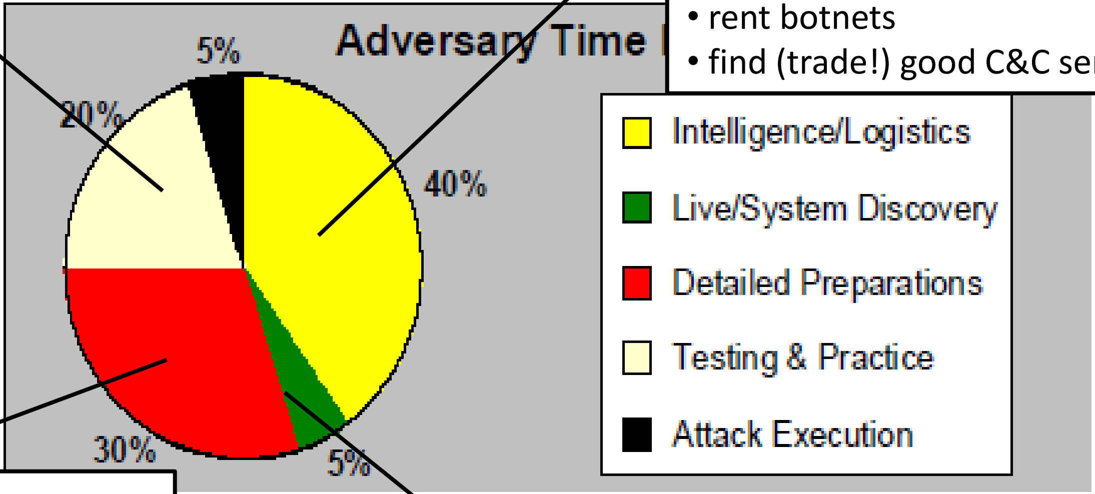
*c) The attack is conducted by a Country C who has hijacked the proxy network? (**False Flag Cyberwar**)*

→ Putting all together

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

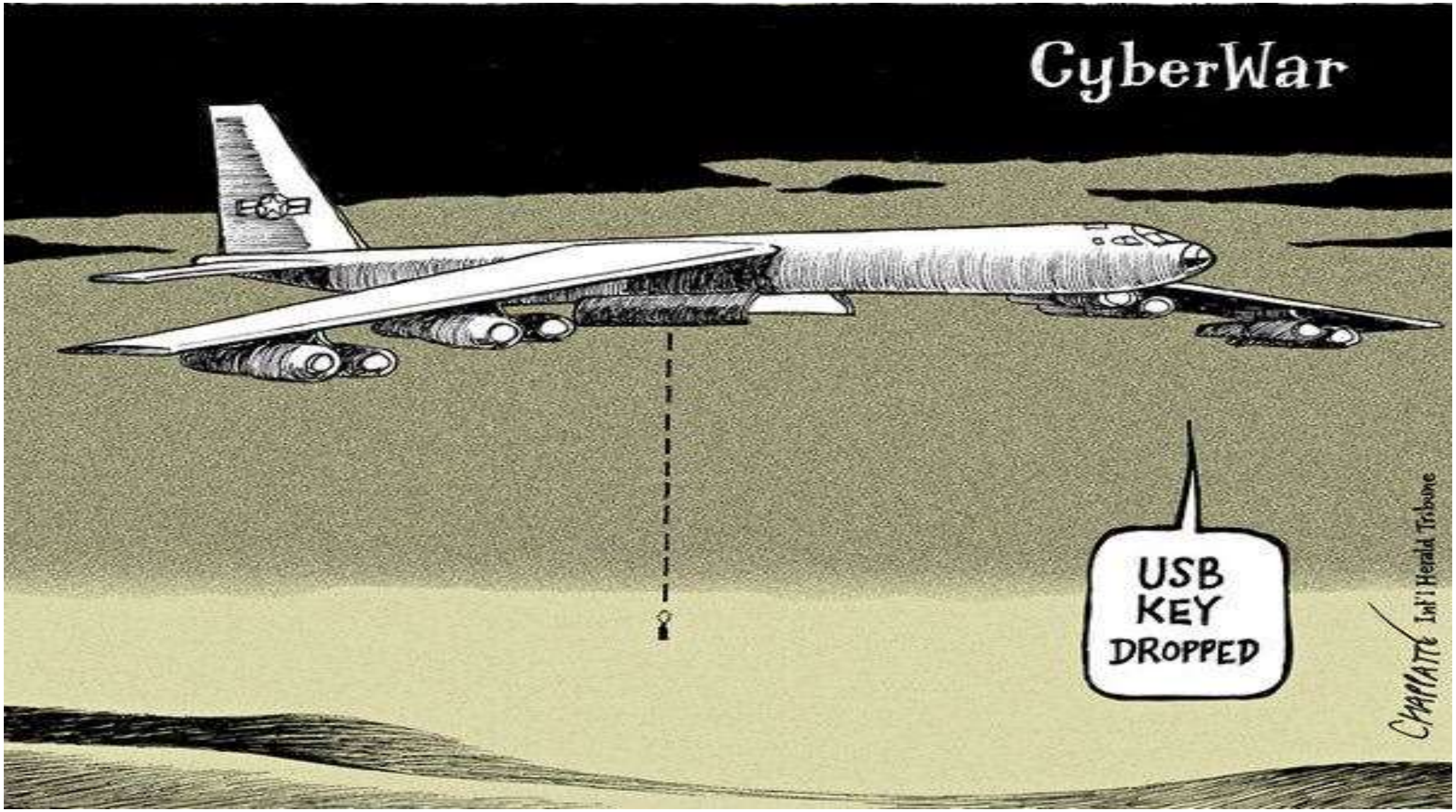


- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

Alexander Klimburg 2012

•Purchase L2/L3 system data

→ It’s not all about a dropped USB key and Stuxnet



→ InfoSec 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?

→ 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

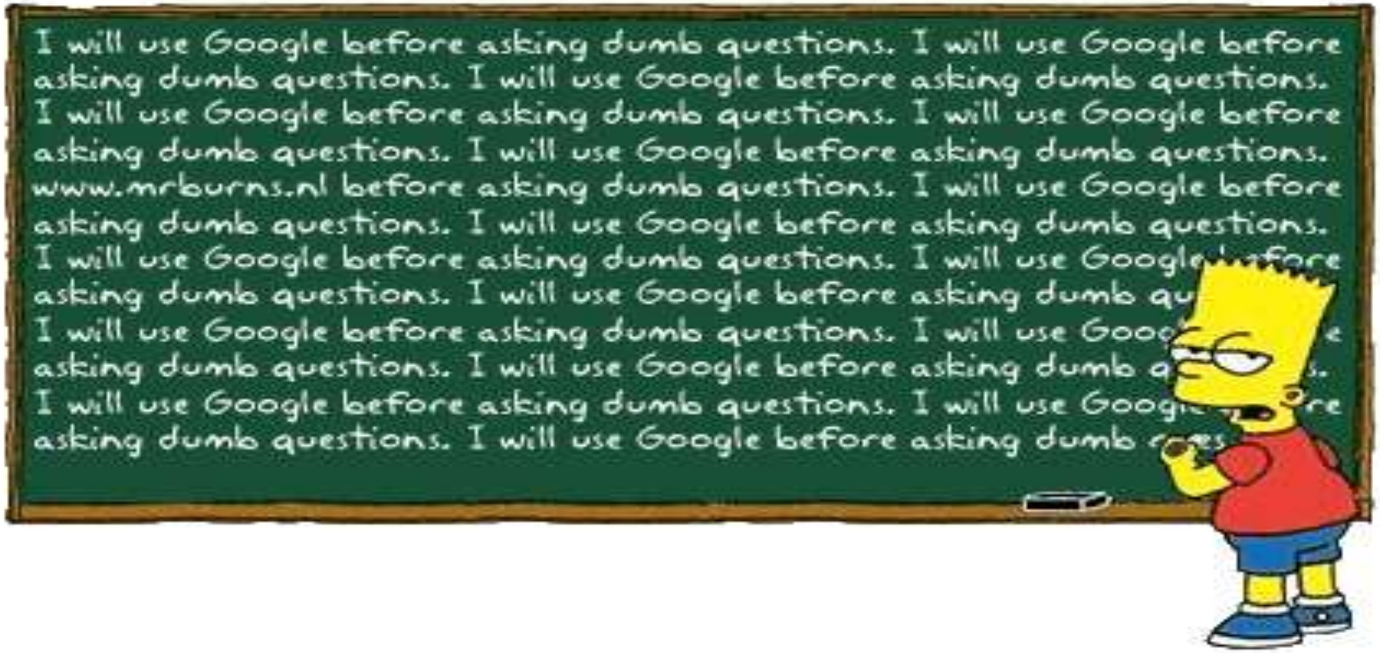
41 http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf

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


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb q
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb

SecurityBrokers
Global Cybersecurity Defense Services

Raoul «nobody» Chiesa

rc@security-brokers.com

GPG Key:
http://cyberdefcon.com/keys/rc.asc