“Cyber cyber cyber Warfare”: mistakes from MoDs.






Raoul «Nobody» Chiesa

Founder, President, **Security Brokers**

Principal, **CyberDefcon Ltd**.

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

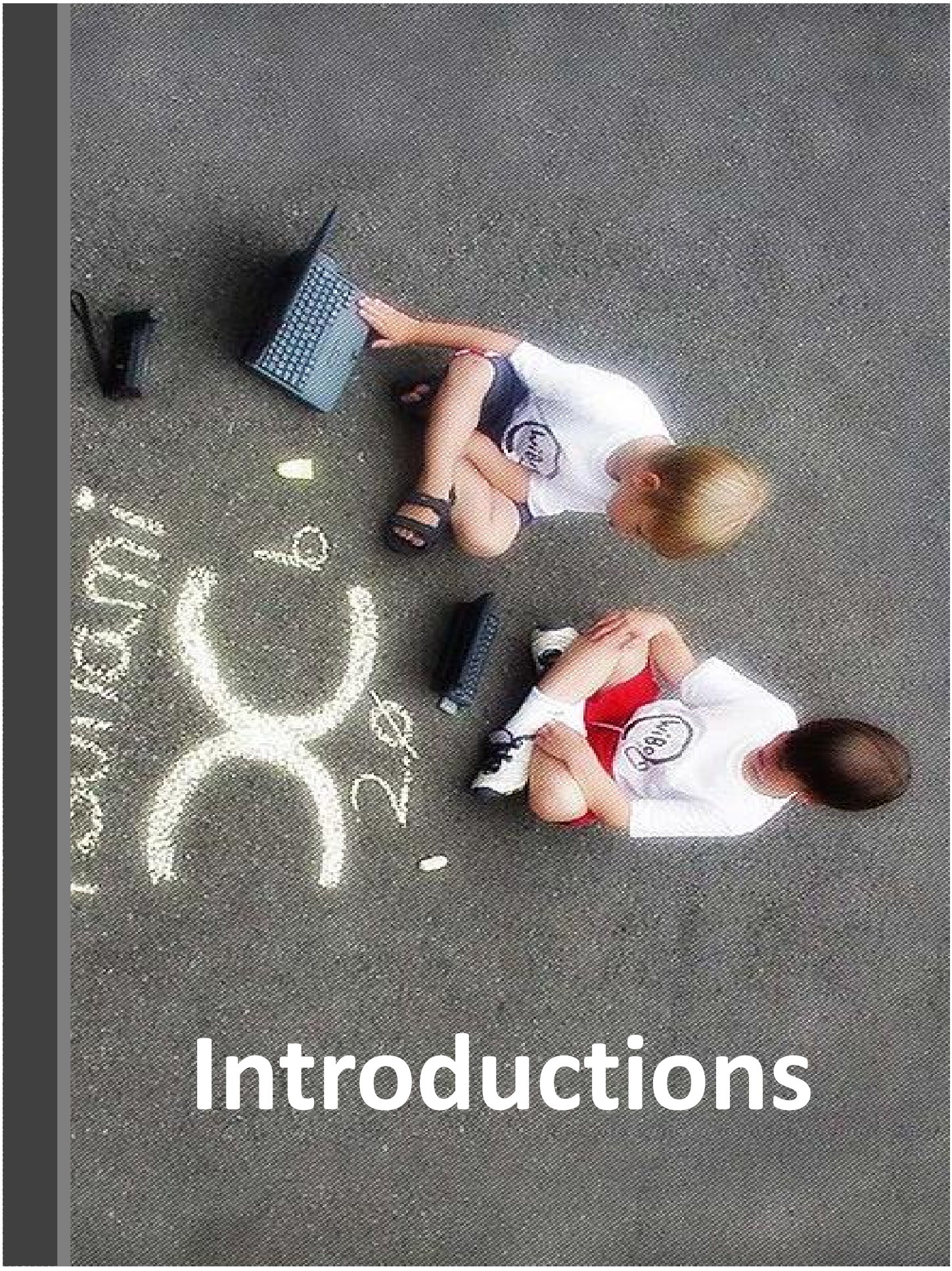
DeepSec 2015, November 19-20, Vienna, Austria

This is the Agenda

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

The views expressed are those of the author(s) and speaker and **do not necessary reflect** the views of NATO, UNICRI, ENISA and/or its PSGs, ISECOM, OWASP, Italian MoD and its WG "Cyber World" at CASD/OSN/CeMiSS, neither the private enterprises and those security communities I'm working at/with and/or supporting.

Thanks for understanding and....**enjoy this presentation** ☺



Introductions

→The Speaker

- Founder, President, @ **Security Brokers SCpA**
- Principal @ **CyberDefcon Ltd.**
- Former 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 Steering Commitee **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Former Member+Co-coordinator of the WG «Cyber World» @ CASD/OSN, **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè, **APWG** European Chapter
- **Roaster of Experts, ITU (International Telecommunication Union)**
- **Supporter at various security communities WW**

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

unicri
United Nations Interregional Crime and Justice Research Institute

CyberDefcon @

Clusit
Associazione Italiana per la Sicurezza Informatica

osn
osservatorio sicurezza nazionale

enisa
European Network and Information Security Agency

ITU

ISECOM

APWG
Committed to Wiping Out Internet Scams and Fraud

OWASP
The Open Web Application Security Project

TEAM CYMRU

I.S.T.F.
Telecom Security Task Force

opsi aip

ICANN

In a nutshell…

- This presentation will (try to) analyze those **mistakes commonly done by MoDs** while **dealing with** the so-called "**Cyberwar**".
  - *Cyberwar is not a terminology I agree with, since it's not regulated (could it be, ever?).*
  - *Instead, I prefer to speak about "Information Warfare" or, "Information Offensive Operations".*
- During this presentation I will pass through **cultural**, **practical**, **logistics** and **narrow-minds issues** I've been able to **observe** in the **last five years**, while **training various military units** in **different countries**.

Ah, and about the “Cyber-cyber-cyber” thing!

- A couple of weeks ago we ran the “Wine Hat” conference in Turin, Italy (winehat.net).
- Despite each speaker’s introduction come with a (specific) bottle of wine, we had a nice rule:
  - *If spelling any word with the prefix “Cyber”, the speaker has to drink the glass of wine.*
- I wasn’t sure if the DeepSec had something similar…. That’s why, in order to “avoid possible exposures”, I put “Cyber x 3”, LOL ☺

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 person said something which has been definitely undervaluated**

"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?**

And much, much more.

We know it.

You know it.

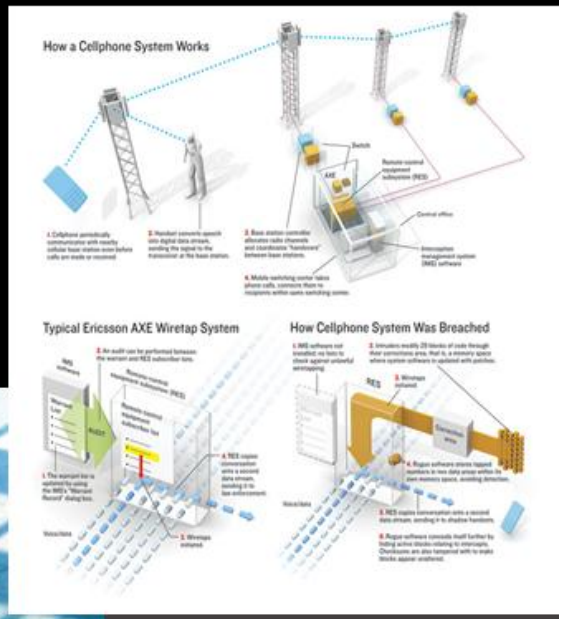
Right?

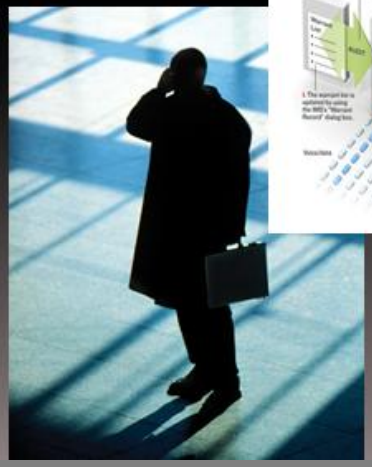
→ **Hmmm… are we missing something? What's the border between INT and MIL games?**

❑ Vodafone Greece 2004 ("The Athens affair")

- ✓ Rootkit on MSC Ericsson AXE
- ✓ Inbound and Outbound Voice calls, SMS in/out, forwarded to 14 "pay-as-you-go" SIM cards (anonymous ones)
- ✓ Olympic Games
- ✓ 14 DEC 2007: Vodafone GR fined with 76M€
- http://spectrum.ieee.org/telecom/security/the-athens-affair
- http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005

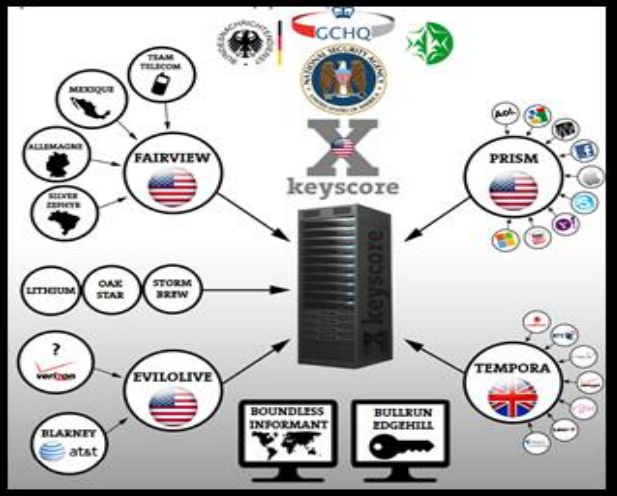
The illegally wiretapped cellphones in the Athens affair included those of the prime minister, his defense and foreign affairs ministers, top military and law enforcement officials, the Greek EU commissioner, activists, and journalists.





→ **Hmmm… are we missing something? What's the border between INT and MIL games?**

- PRISM and other secret project's scandals ("the Snowden case")
- NSA's budgets for black operations revealed
  - http://rt.com/usa/snowden-leak-black-budget-176/
  - http://rt.com/usa/us-hacking-exploits-millions-104/
  - http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
  - http://www.repubblica.it/tecnologia/2013/08/31/news/sall_nsa_231_cyber-attacchi_nel_2011_cos_colpiva_l_intelligence_americana-65600302/



→ **Hmmm… are we missing something? What's the border between INT and MIL games?**

- NSA's "black budget": 652M$ (2011)
- 231 black operation until today (2011)
- 16 US agencies involved from the US Intelligence community (107.035 employees)

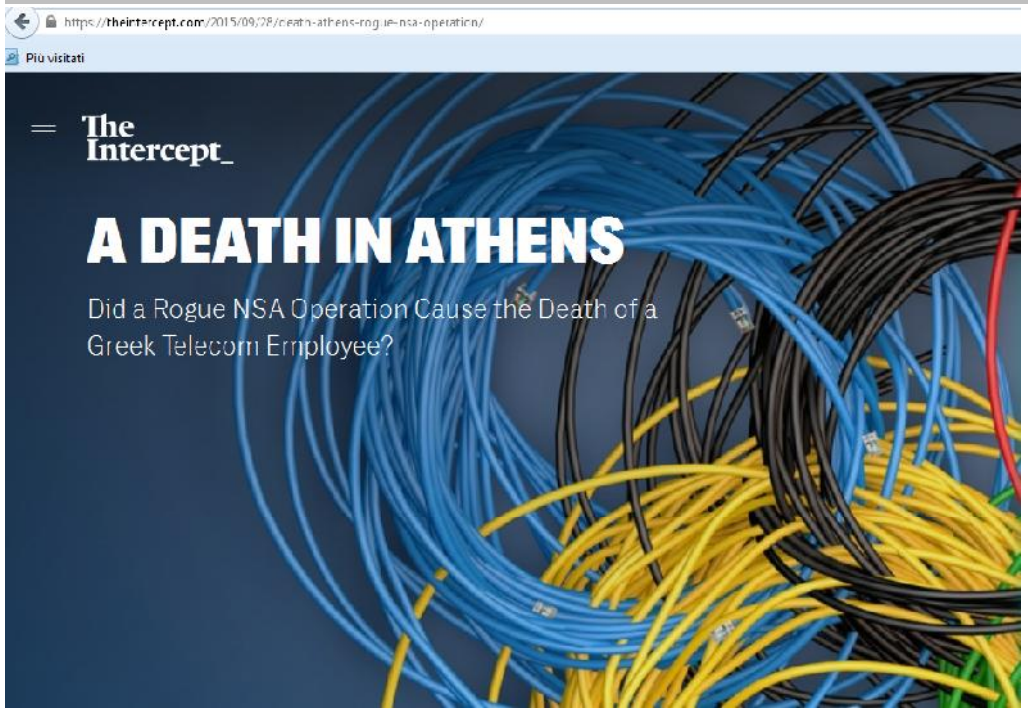
- Targets: US intelligence agencies high priority:
  - ✓ Iran
  - ✓ Russia
  - ✓ China
  - ✓ Afghanistan
  - ✓ North Korea
  - ✓ Syria
  - ✓ ……

The Washington Post

- Cyber Attacks Unit "GENIE"

- Hacking into foreign systems in order to spy on contents, controlling functions
- http://articles.washingtonpost.com/2013-08-29/world/41709796_1_intelligence-community-intelligence-spending-national-intelligence-program

→ **Hmmm… are we missing something? What's the border between INT and MIL games?**



Costas Tsalikidis, Network Planning Manager, Vodafone Panafon

Vodafone Greece CEO George Koronias holds documents in April 2006 before the start of a parliamentary committee hearing investigating the phone-tapping scandal.
Photo: Louisa Gouliamaki /AFP/Getty Images

→ Hmmm… are we missing something? What's the border between INT and MIL games?

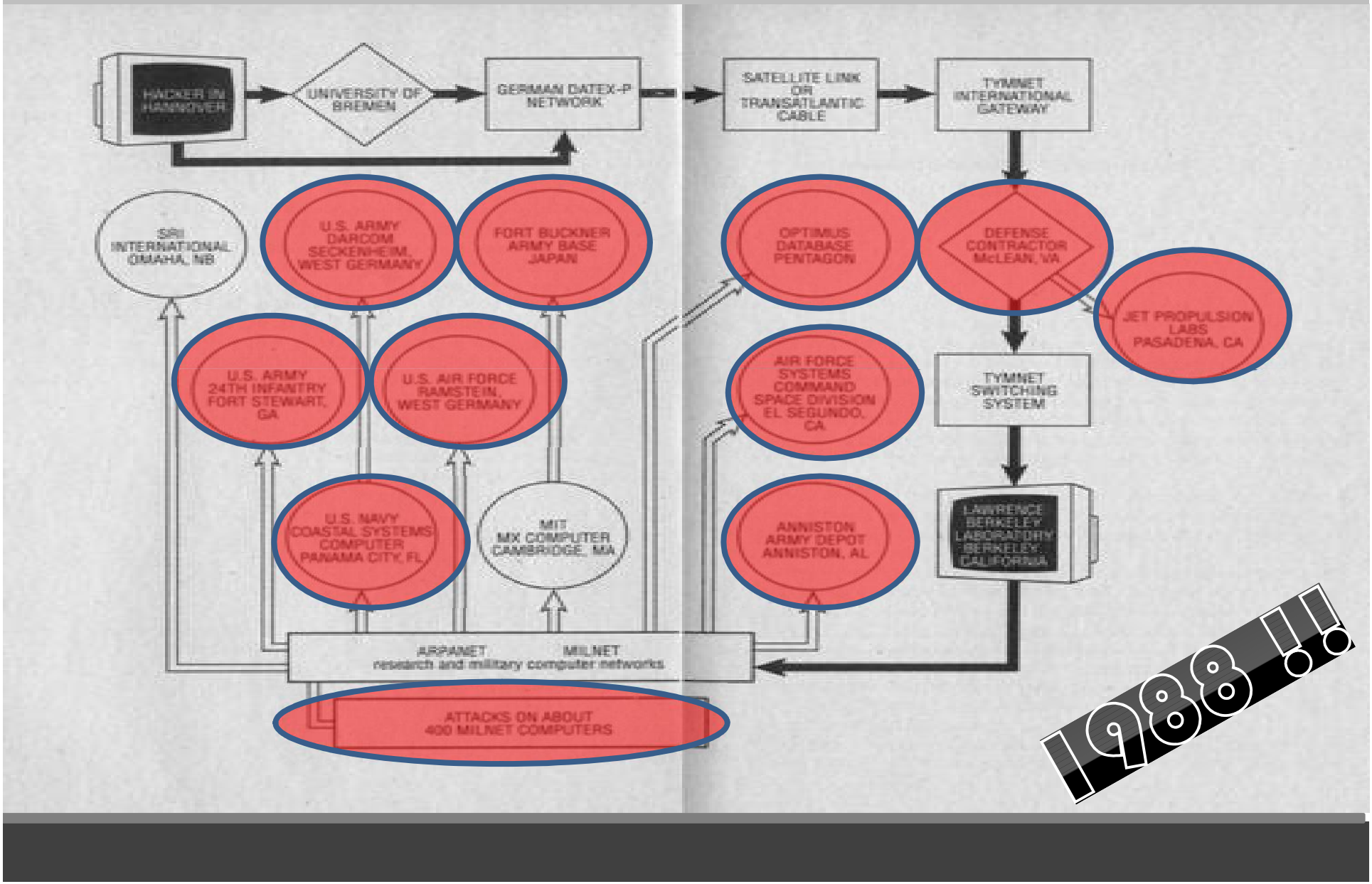
Belgian Telco says it was hacked, while reports point to NSA or GCHQ as culprit

http://gigaom.com/2013/09/16/belgian-telco-says-it-was-hacked-while-reports-point-to-nsa-or-gchq-as-culprit/

→ So, is all of this a «fresh» approach? NO!

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

→ **Back to the 80's…**

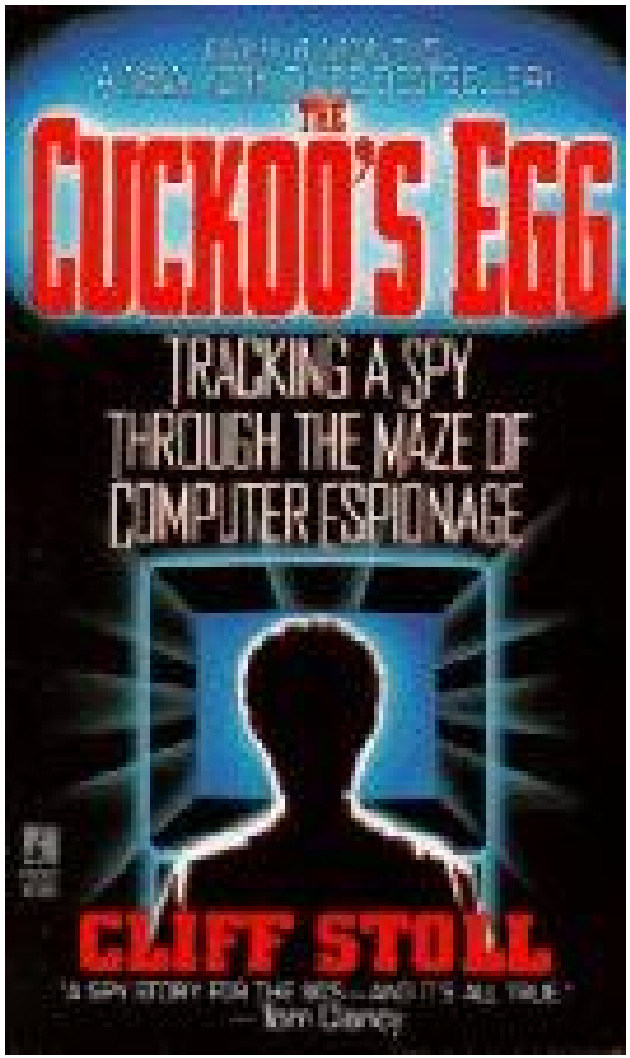


→ **Back to the 80's…**

- 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?**



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

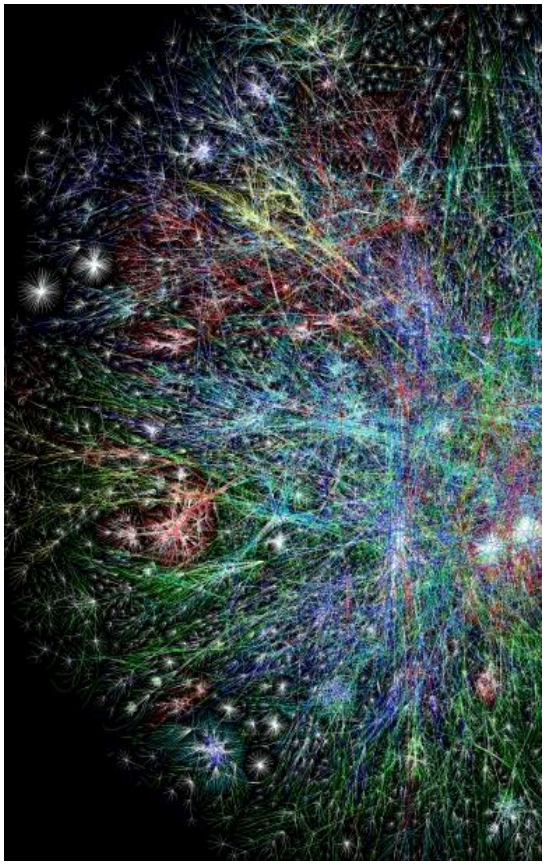
Remotely done = Cyber INT

→ In real life: WHO is doing WHAT?

Cyberwarfare has a **very wide spectrum of action** and uses **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
- ICs / LEAs / MILs
- Organized Cybercrime
- Hacktivists
- Industrial Spies
- Terrorists
- Corporations
- Cyber Mercenaries

Everyone against everybody



→ 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)
- Actors background have changed, definitely
  - 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-attacks in order to:
  - Industrial Espionage (with a Intelligence or a Military approach)
  - Information manipulation
  - Supporting real-life operations
  - Cyber-warfare and cyber-weapons


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)

unicri
advancing security, serving justice, building peace

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)**

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** (AFAIK, all of 'em are located in Eastern Europe)

Nations Wordwide Status

→ I found this in 2004…

Summary of nation-state cyberwarfare capabilities

	China	India	Iran	N. Korea	Pakistan	Russia
Official cyber-warfare doctrine	X	X			*Probable*	X
Cyberwarfare training	X	X	X		X	
Cyberwarfare exercises/simu-lations	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 hack-ing 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	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)

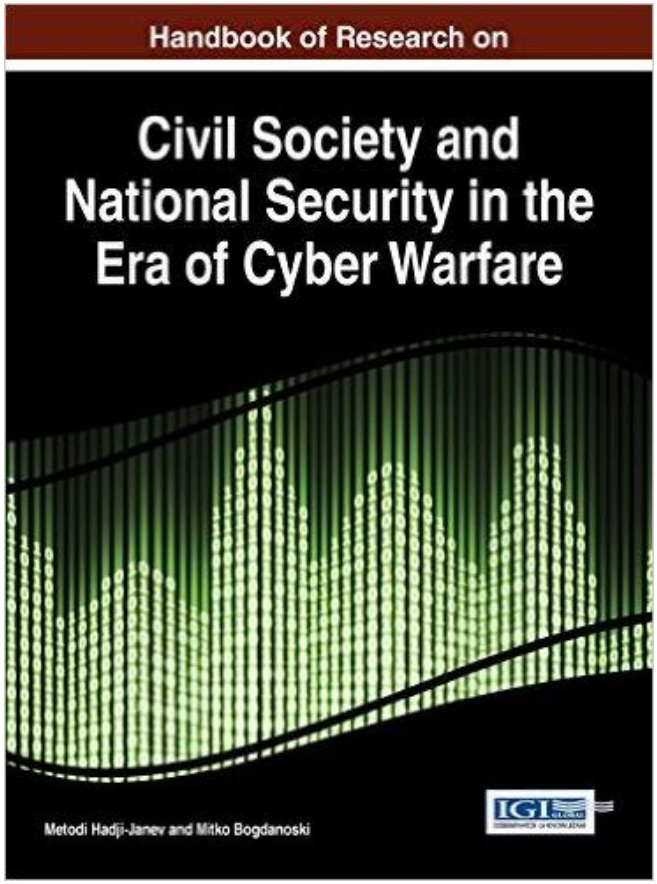
Nations with Cyber Defense Capabilities / 2

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	

→ GET the FULL updated (NOV 2015) research from chapter #9 of this book (just published):

Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare (Advances in Digital Crime, Forensics, and Cyber Terrorism) 1st Edition

ISBN-13: 978-1466687936
ISBN-10: 1466687932



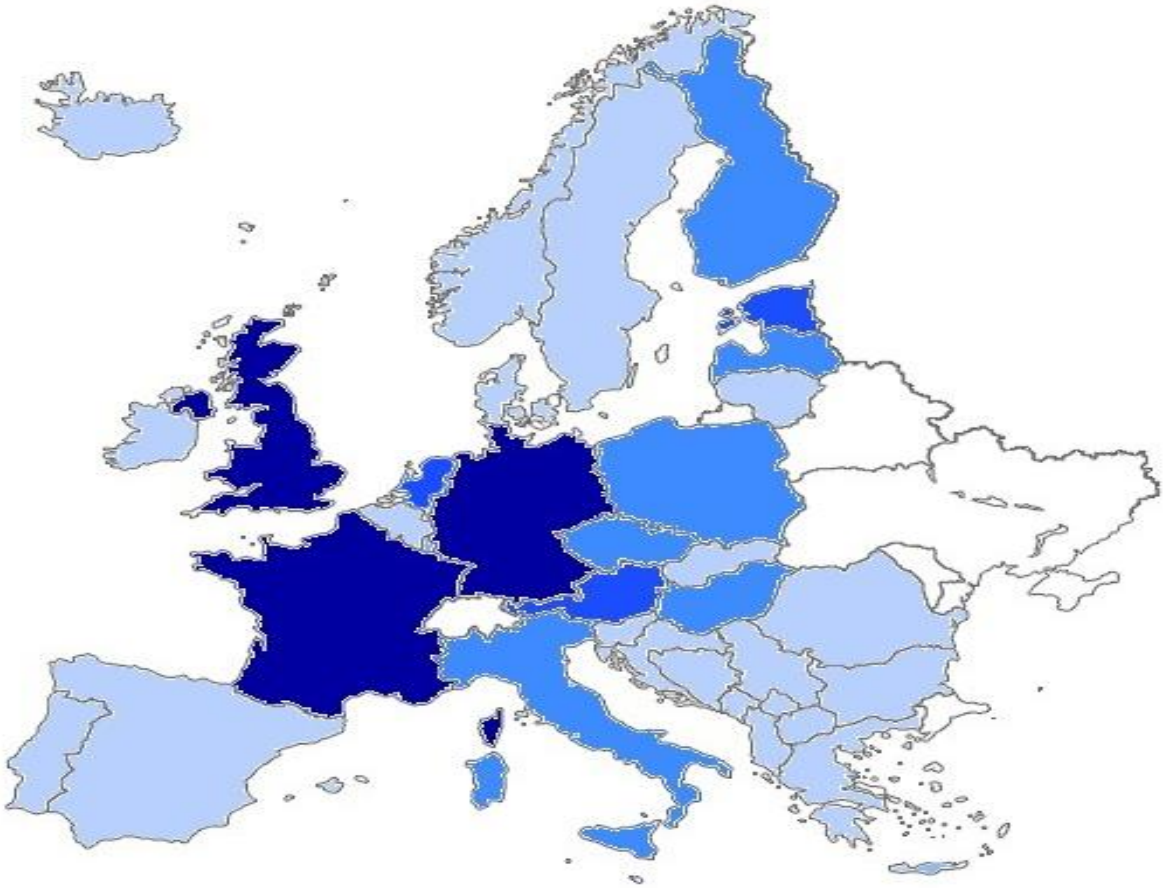
http://www.igi-global.com/book/handbook-research-civil-society-national/129591

→ 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…

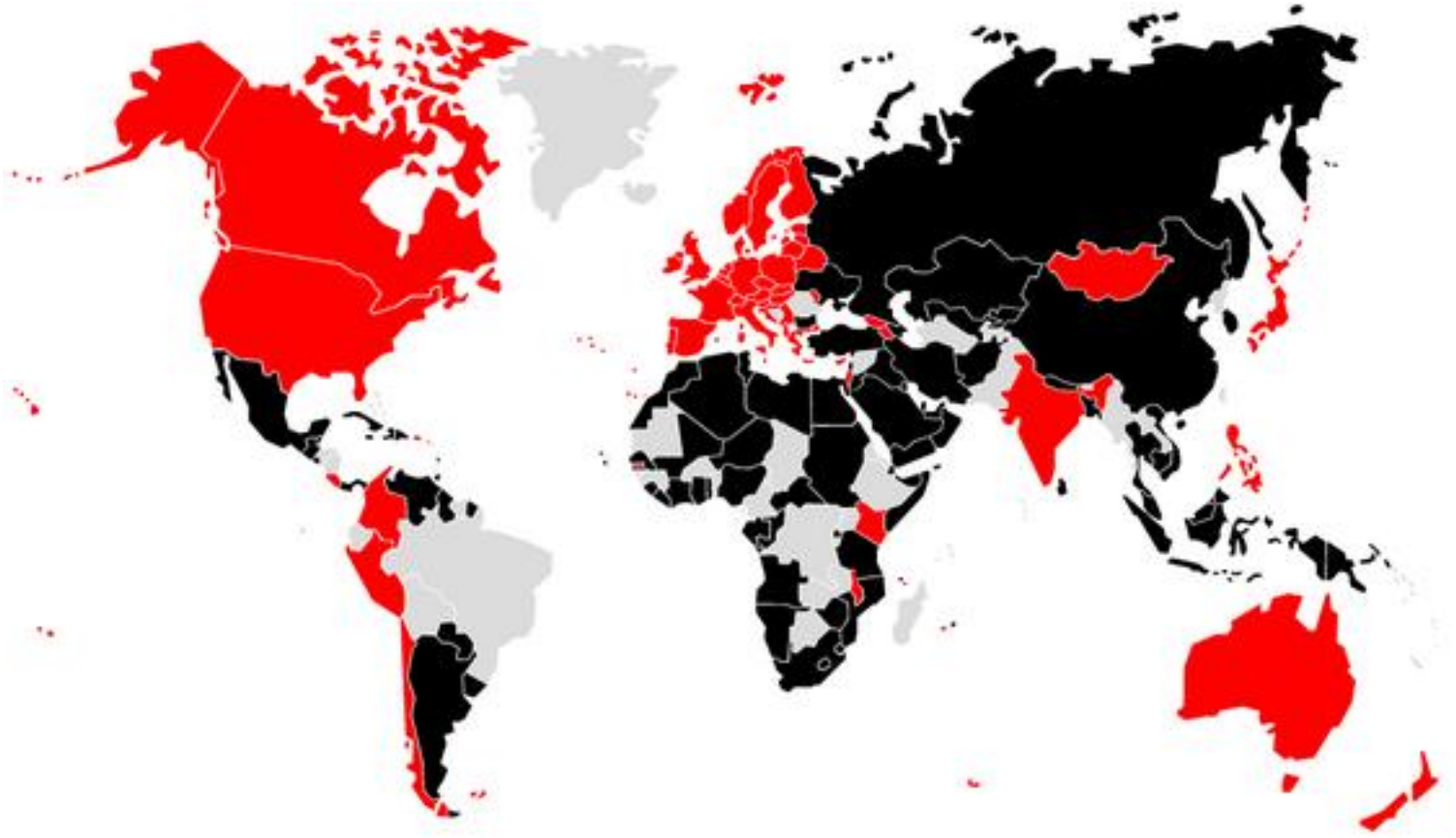
1. **Generational problem**: Generals are too old, often they don't speak English and they don't really know the topic. Younger officials don't have the needed decision-power.
2. **Terminology** problems: «cibernetic» to us means something else… ☺
3. Lack of *internationally-agreed* **laws** on «cyber 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 jets, 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.

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



Source: Flavia Zappa,
Security Brokers, 2013

→ 2013 - Map of ITU Dubai General Assembly December 2012 (red=not signed; black=signed)



Source: Flavia Zappa, Security Brokers, 2013

- "Cyberwar" is real, but it might not be what *you* think;
  - most of what we call "cyberwar", as a community and the media, 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 behavior** 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)***

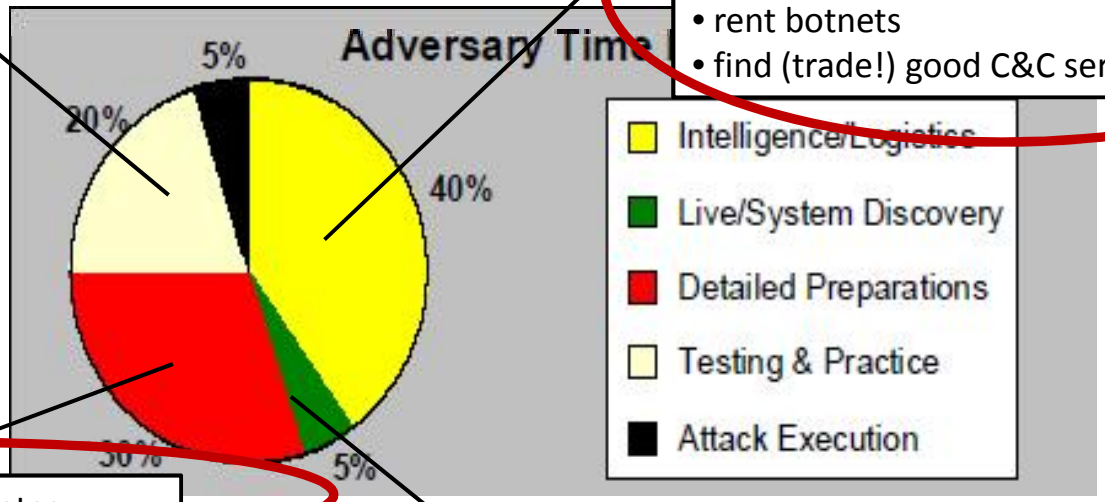
c) *The attack is conducted by a Country C who has hijacked the proxy network?* ***(False Flag Cyberwar)***

→ **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

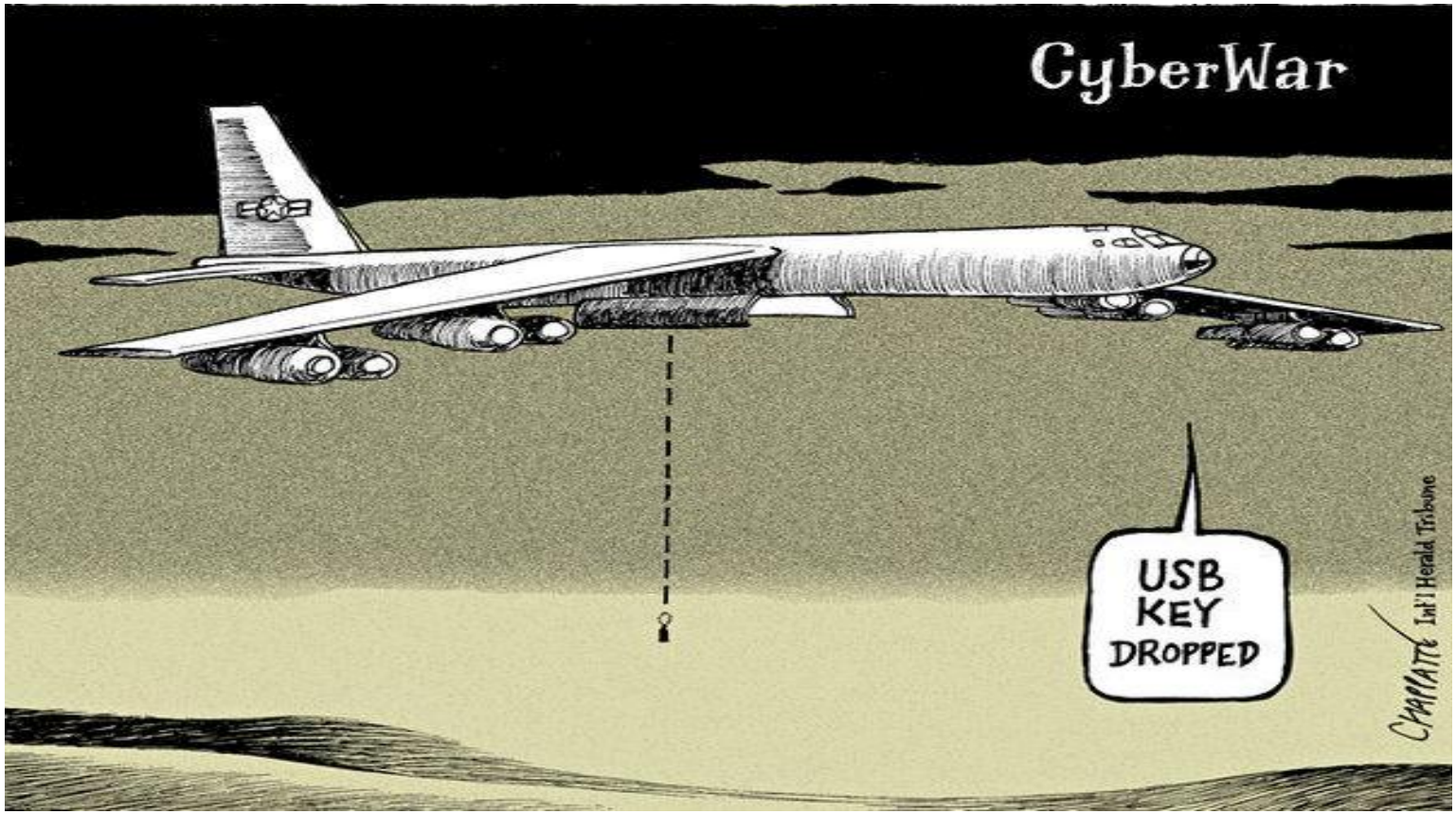


- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

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?

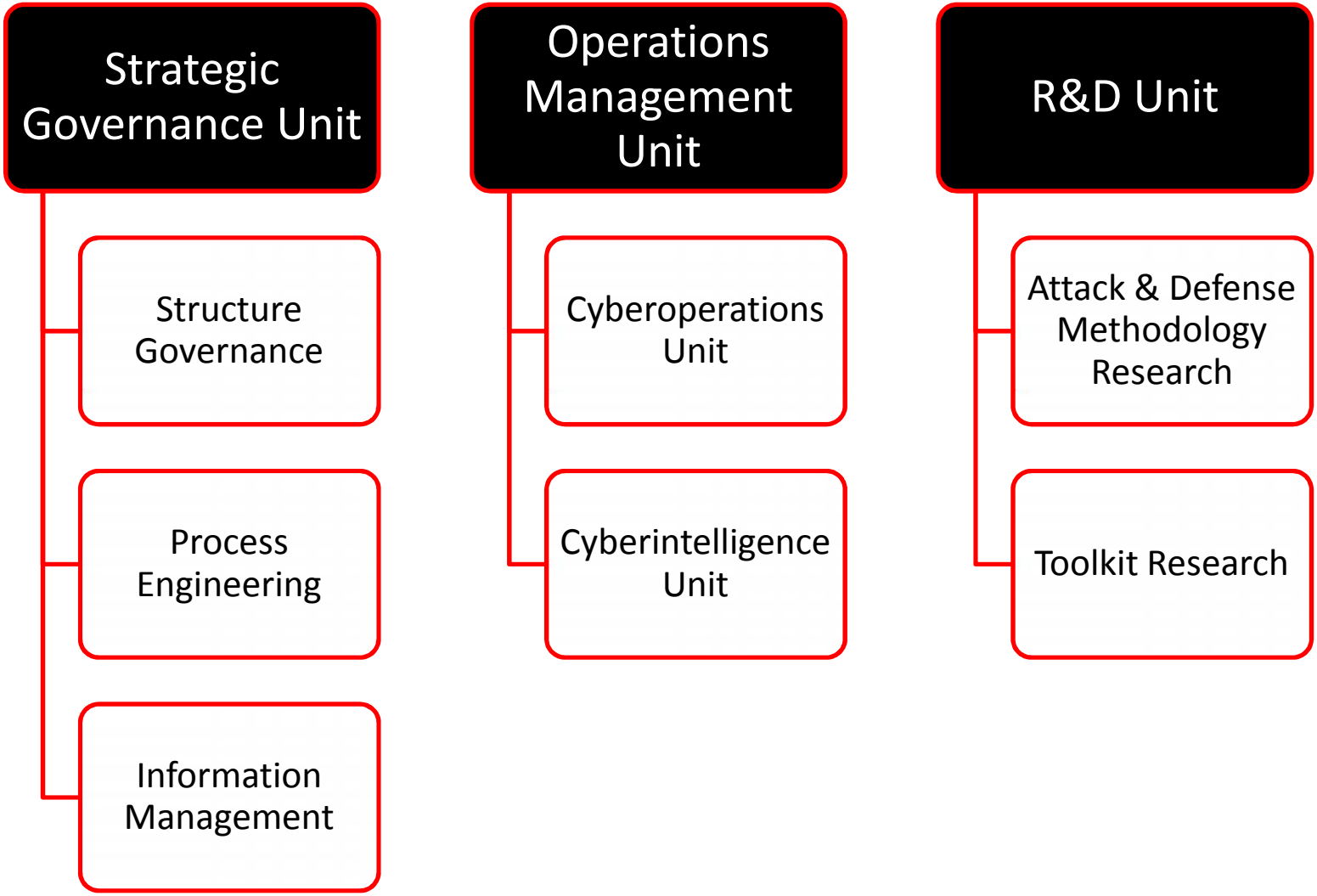
- **Digital Offense capabilities** as a **key factor** for **effective digital cyber warfare**.
- **Provide cyberspace-wide support** for *civil* and *military* **intelligence operations**.
- **Real world digital attacks** are not just "Penetration testing".

Offensive Security: recruiting

- Recruiting “digital soldiers” 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



- 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**.

→ 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

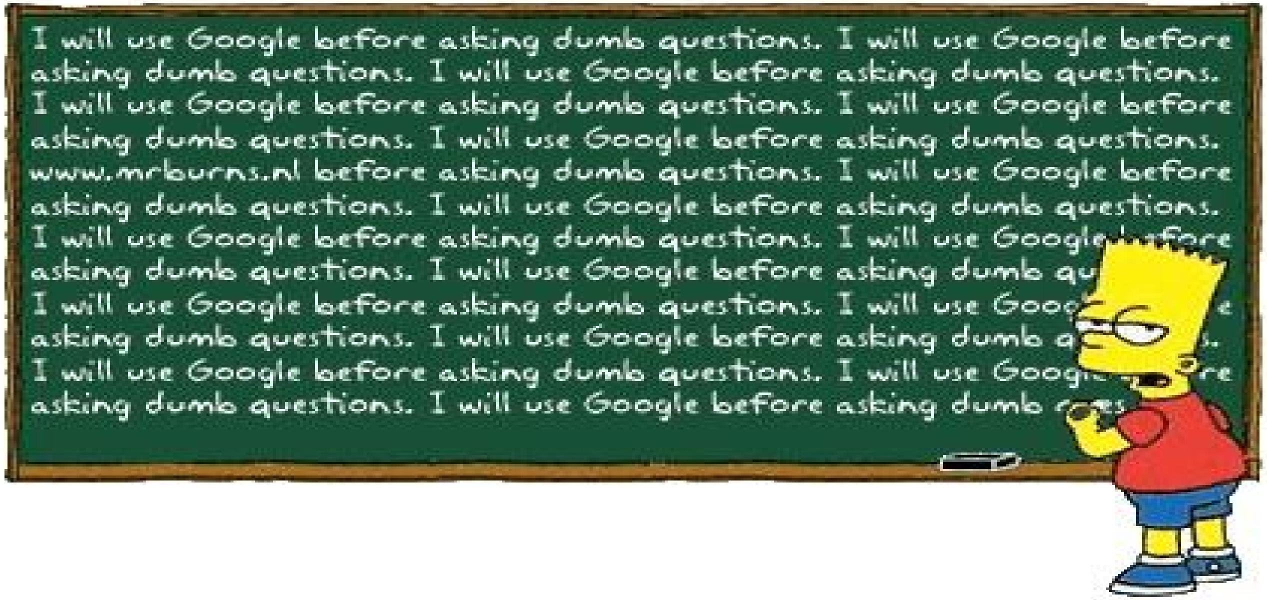
[40] http://www.defense.gov/news/newsarticle.aspx?id=65739

[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



Raoul «nobody» Chiesa

rc [at] security-brokers [dot] com

GPG Key: https://www.security-brokers.com/keys/rc_pub.asc

SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES