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

Raoul «Nobody» Chiesa

Founder, Partner, **The Security Brokers**

Principal, **CyberDefcon Ltd.**

Partner, **TSTF**

SecurityBrokers
Global Cybersecurity Defense Services

TSTF .net
Telecom Security Task Force

CyberDefcon

This is the Agenda!

- The speaker
- Scenarios
  - What’s outta there?
  - Definitions w/ a plausible case study/scenario
- Nation’s worldwide status
  - Hot players (countries)
  - Hot players (privatization)
- Building your own Cyber Army
  - General model
  - Business model
  - Operating model
  - Costs analysis
  - Attack Operations….opsss! I mean «Offensive Behaviour! - Costs & Timeframes
- A (theorical?) case study – Airports all over the world!
- Conclusions
- Credits, Contacts, Q&A

Disclaimer

→Disclaimer

- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of UNICRI, ENISA and its PSG, nor the companies and security communities I'm working at and/or supporting.

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

- **Thank you** and....**enjoy this talk** ☺

Introductions

→The Speaker

Raoul Chiesa

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

Scenarios

→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

→..in order to study the present…

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

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

"2011 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

Various sources (UN, USDOJ, INTERPOL, 2011)

Financial Turnover, <u>estimation</u>: 6-12 BLN USD$/year

Source: Group IB Report 2011

http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf

GROUP IB

State and trends of the "Russian" computer crime market in 2010

„Cybersecurity, Cyber-security, Cyber Security ?"

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?

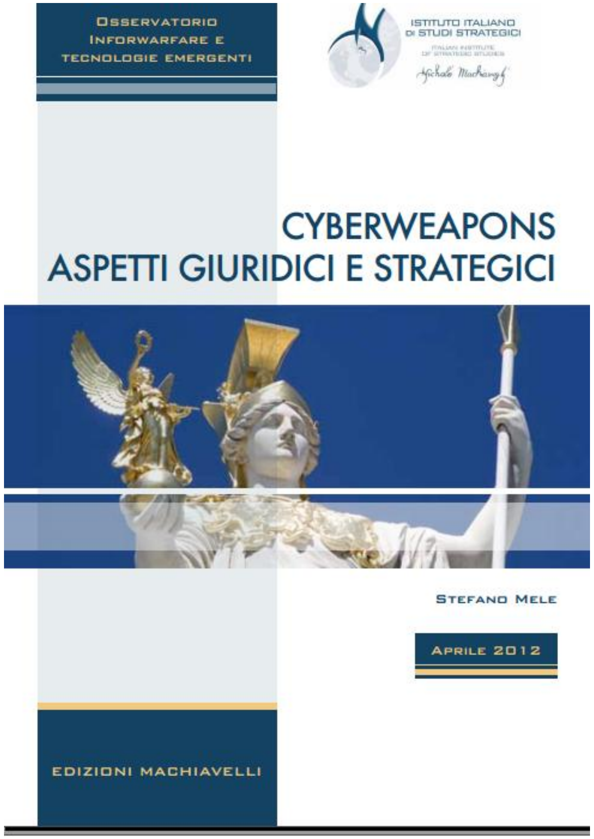
→ Definition of «cyberweapon»

- Nevertheless, (cyber-)lawyers looks to live one step ahead (WOW!) in this case.

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

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

(Source: http://hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/ and http://www.strategicstudies.it/wp-content/uploads/2011/10/Paper-Apr-2012_Cyberweapons.pdf)



OSSERVATORIO INFORWARFARE E TECNOLOGIE EMERGENTI

ISTITUTO ITALIANO DI STUDI STRATEGICI

ITALIAN INSTITUTE OF STRATEGIC STUDIES

Niccolò Machiavelli

CYBERWEAPONS
ASPETTI GIURIDICI E STRATEGICI

STEFANO MELE

APRILE 2012

EDIZIONI MACHIAVELLI

→ What are we talking about? Why?

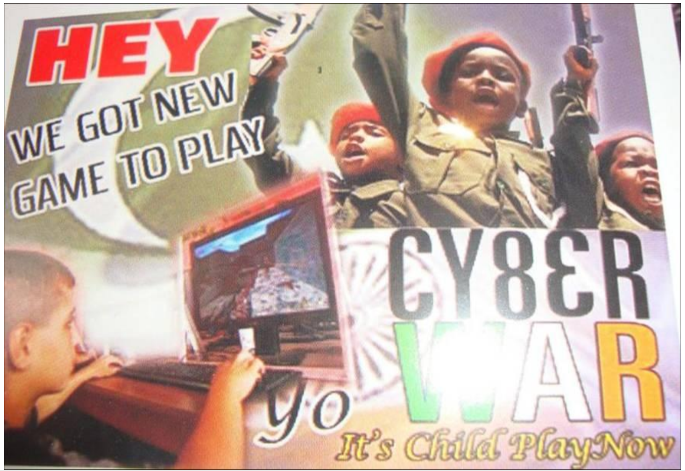
- **Cybercrime** is still very much a problem and of prime important for the LE community.
    - Though not the focal point of my talk!
- **"Cyberwar"** is often confusing and contradictory. Despite being a term **I really don't like**.
    - NOTE: When we use the suffix, "-war" appended to "cyber", we do not mean to use that term lightly or belittle the toll it can take on humanity. This will be echoed again and again in this talk.
- We are also **not referring to kids** defacing public-facing websites (on one end) or to forcing entire national power grids offline (on the other extreme end of the spectrum).
    - … though that second one is at least *theoretically* possible, focusing exclusively on that stuff is a red herring as you will see (remember the "Brazil hacks"?)
- So **what is "cyberwar"**? Is it the use of networking on the conventional battlefield ("Network-centric warfare")? Is it **espionage** and possibly **sabotage** on an **adversary's infrastructure**? Is it **sabotage directed at an adversary's economic infrastructure**?
    - Why does so much "cyberwar" discussed in the media **look a lot like espionage and spycraft**?

→ Starting from Cybercrime? No, from hacking!

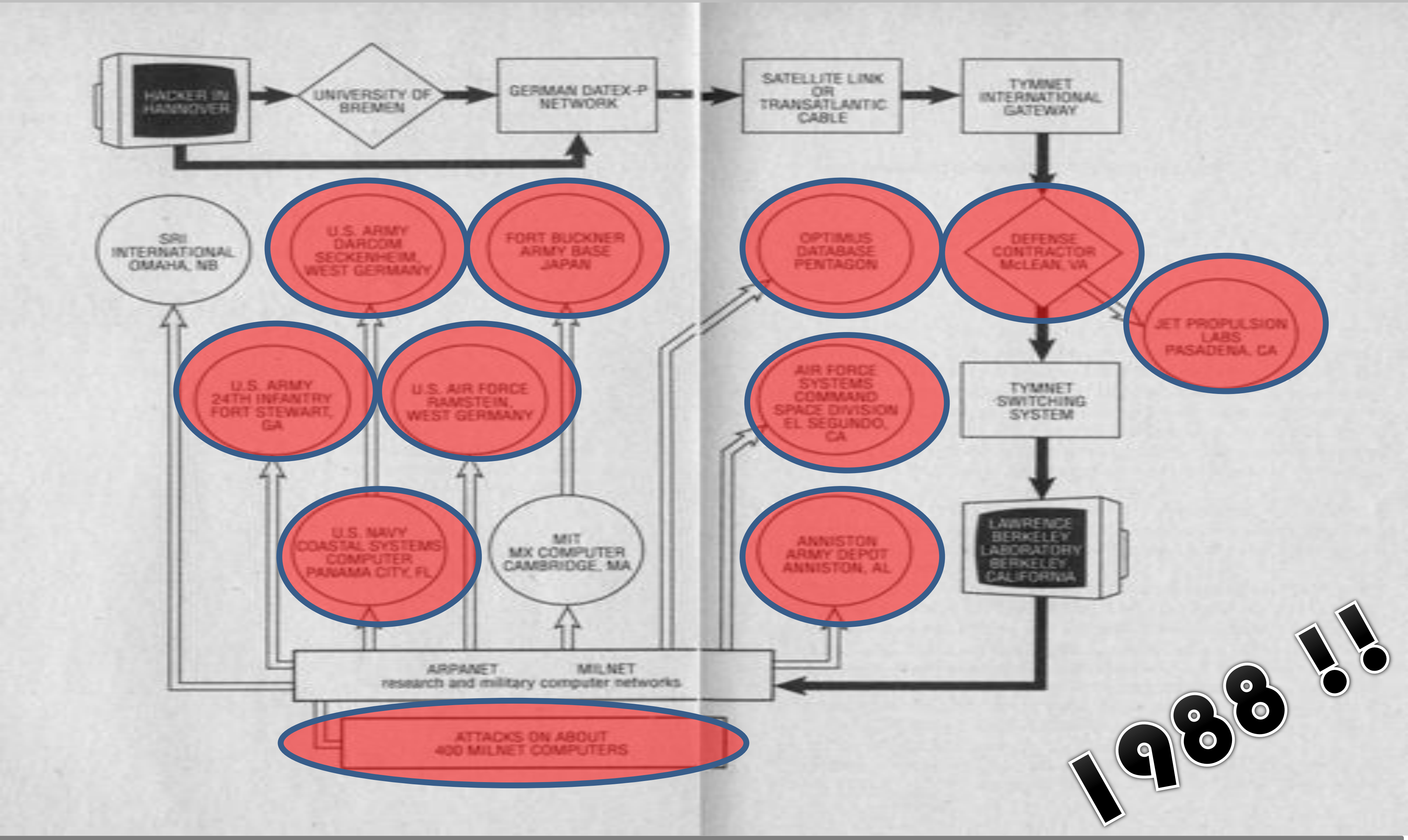
- Before “cyberwar”, there was **cybercrime**.

- But before “cybercrime”, there was **straight-up hacking**.
  - 1980's - independent actors, hacking is very much on the fringe and motivated, for the most part, by curiosity and egoism.

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



→ Back to the 80's...


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

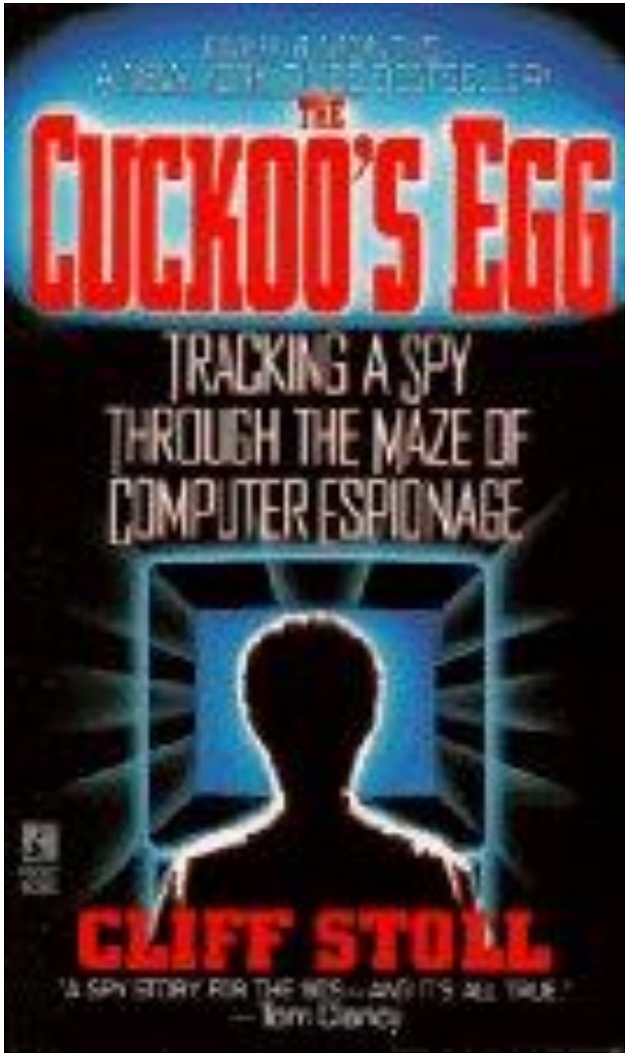
1988 !!

→ 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's hackers Hagbard and Pengo.
  - ✓ Defense Contractor McLean, VA
  - ✓ JPL – Jet Propulsion Labs, Pasadena, CA
  - ✓ LBNL – Lawrence Berkeley National Labs , Berkeley, CA
  - ✓ NCSC – National Computer Security Center
  - ✓ Anniston Army Depot, Anniston, AL
  - ✓ Air Force Systems Command Space Division, El Segundo, CA
  - ✓ OPTIMUS Database, PENTAGON
  - ✓ Fort Buckner Army Base, **JAPAN**
  - ✓ U.S. AIR FORCE, Raimsten, **GERMANY**
  - ✓ U.S. NAVY Coastal Systems Computer, Panama City, FL
  - ✓ U.S. ARMY 24th Infantry, 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 80s... 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 Security
  - ✓ SIGSEC = Signals Security
- C-SIGINT = Counter-Signals Intelligence
- ECM = Electronic Countermeasures
- EMI = Electromagnetic Interference
- IBW = Intelligence-based Warfare
- IEW = Intelligence and Electronic Warfare

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

→ A jump to 2007…

"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers.

This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces.**"**

Former Duma speaker Nikolai Kuryanovich, 2007

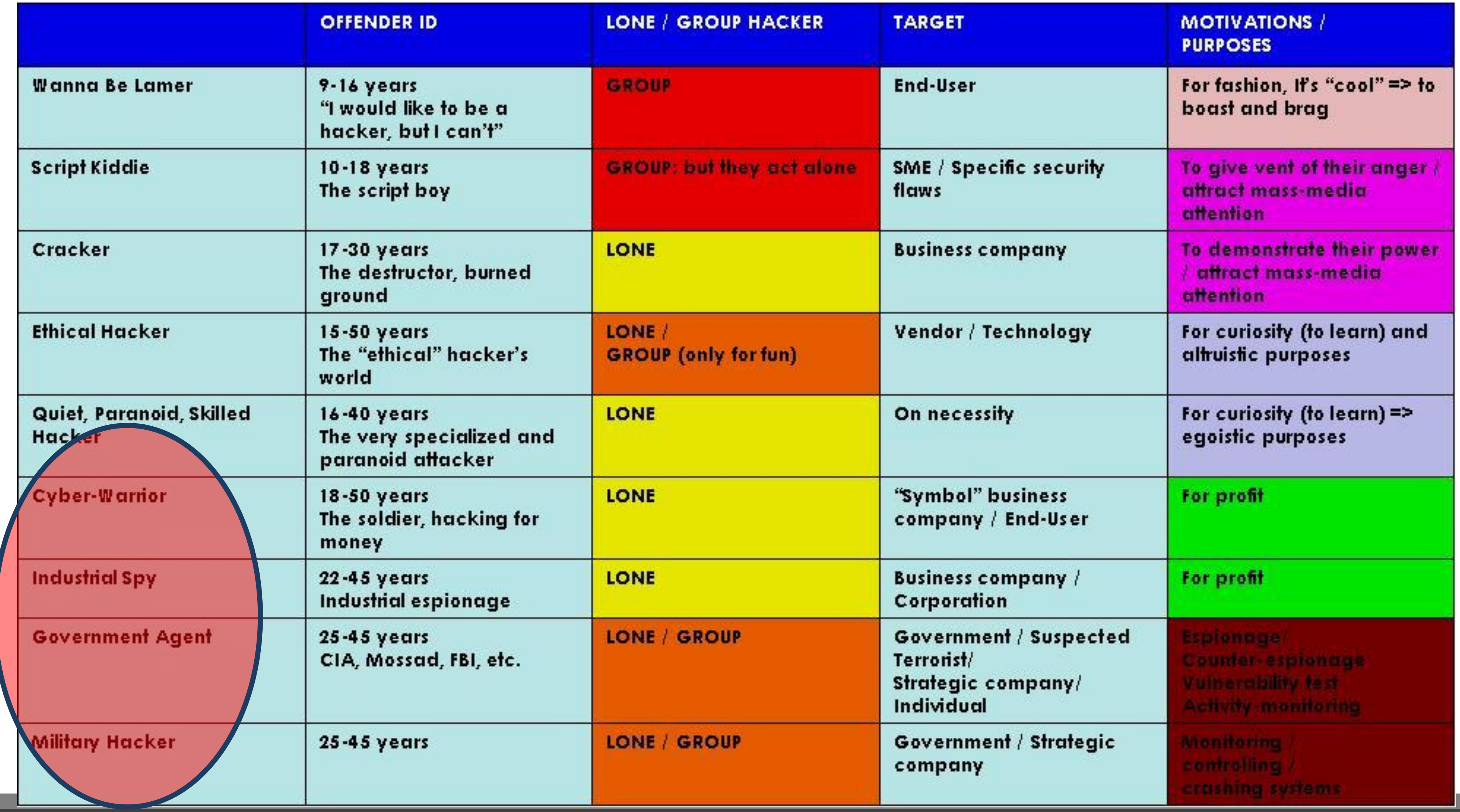
→ So, what do I see in the next years ☺ LOL!!

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

→ Profiling «Hackers» (United Nations, UNICRI, HPP V1.0 – 2004-2010)

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

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

→ **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."

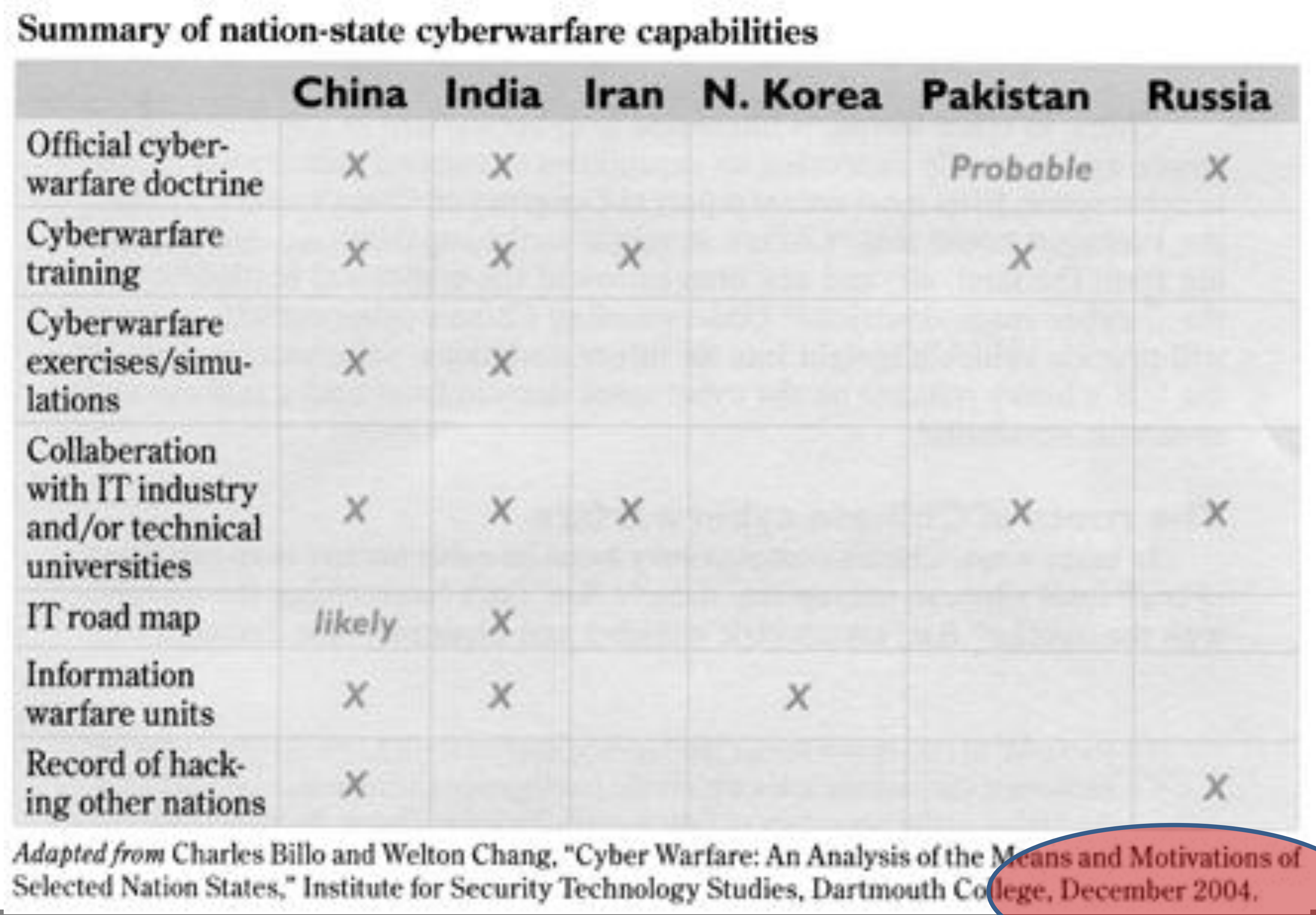
How does country B know if:

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**)*

→ Back some years ago…



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/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.

→ 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	

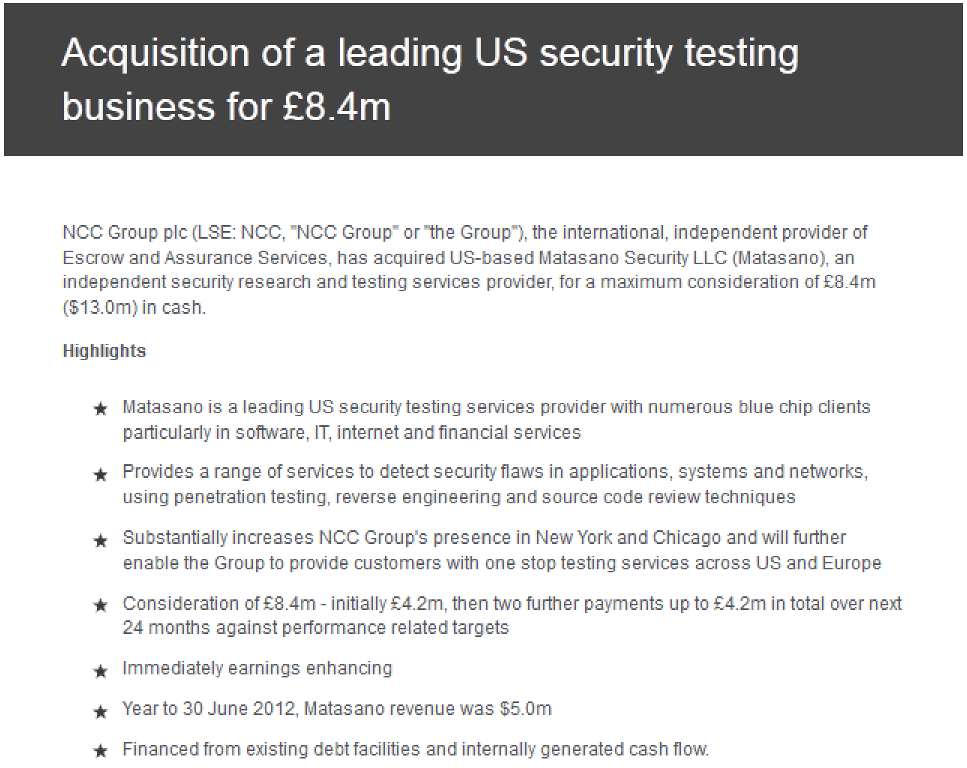
→ The right words

- “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, as I will illustrate, **a lot of the assets and techniques** used in (cyber) criminal or (cyber) espionage operations **can easily scale upwards to be used** within warfare scenarios.
    - Let’s not forget there are **alternate means of changing a state’s behaviour** beyond “war”: economics, diplomatic issues, informational advantages…

- I prefer the term "**information operations**" as that is what **most cases of today refer to**, but "cyberwar" **gets the attention of both media and financial planners**. So be it.

→ Privatization of «cyber-*»

- And of course, in true Anglo-Saxon model, private enterprise emerged to fill the void… **prompting a wave of buy-outs and re-alignments:**



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

NCC Group plc (LSE: NCC, "NCC Group" or "the Group"), the international, independent provider of Escrow and Assurance Services, has acquired US-based Matasano Security LLC (Matasano), an independent security research and testing services provider, for a maximum consideration of £8.4m ($13.0m) in cash.

Highlights

★ Matasano is a leading US security testing services provider with numerous blue chip clients particularly in software, IT, internet and financial services

★ Provides a range of services to detect security flaws in applications, systems and networks, using penetration testing, reverse engineering and source code review techniques

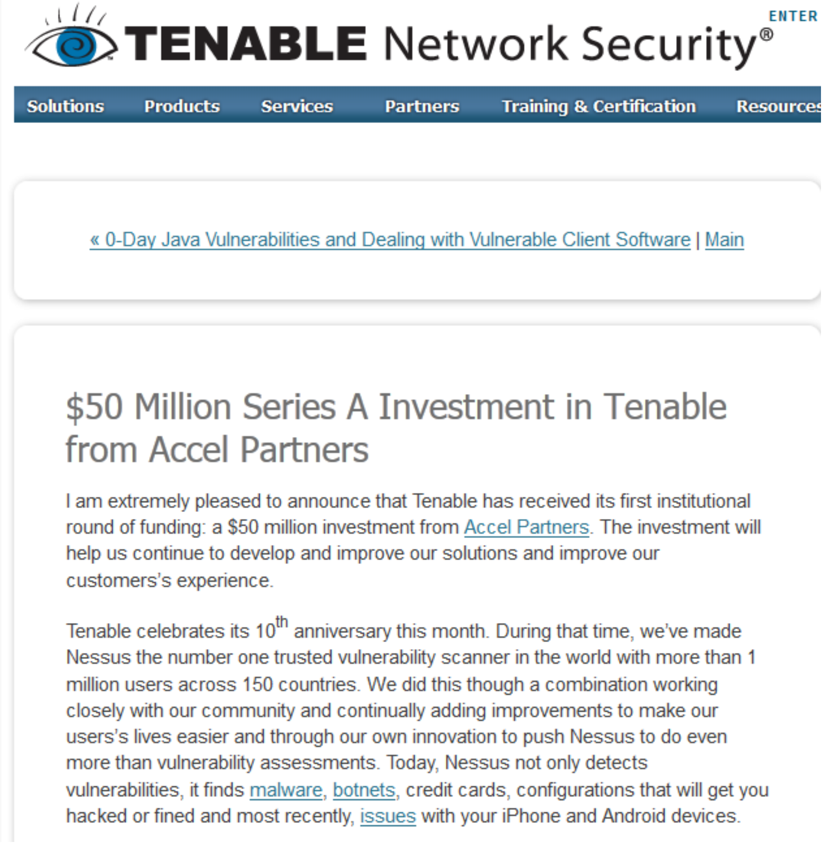
★ Substantially increases NCC Group's presence in New York and Chicago and will further enable the Group to provide customers with one stop testing services across US and Europe

★ Consideration of £8.4m - initially £4.2m, then two further payments up to £4.2m in total over next 24 months against performance related targets

★ Immediately earnings enhancing

★ Year to 30 June 2012, Matasano revenue was $5.0m

★ Financed from existing debt facilities and internally generated cash flow.



« 0-Day Java Vulnerabilities and Dealing with Vulnerable Client Software | Main

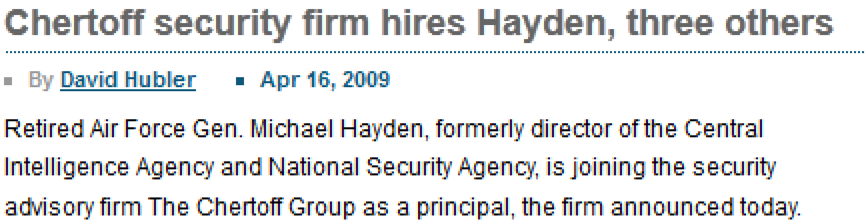
$50 Million Series A Investment in Tenable from Accel Partners

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

Tenable celebrates its 10th anniversary this month. During that time, we've made Nessus the number one trusted vulnerability scanner in the world with more than 1 million users across 150 countries. We did this though a combination working closely with our community and continually adding improvements to make our users's lives easier and through our own innovation to push Nessus to do even more than vulnerability assessments. Today, Nessus not only detects vulnerabilities, it finds malware, botnets, credit cards, configurations that will get you hacked or fined and most recently, issues with your iPhone and Android devices.

→ Privatization of «cyber-*»

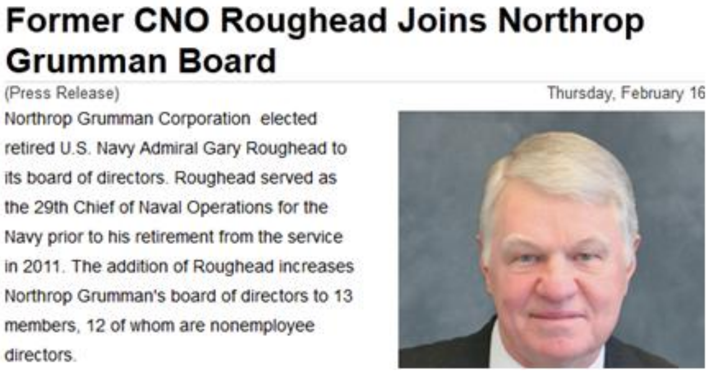
- And of course, in true Anglo-Saxon model, private enterprise emerged to fill the void... **prompting a wave of “lateral movement” of state workers to the private sector:**



Chertoff security firm hires Hayden, three others

By David Hubler ▪ Apr 16, 2009

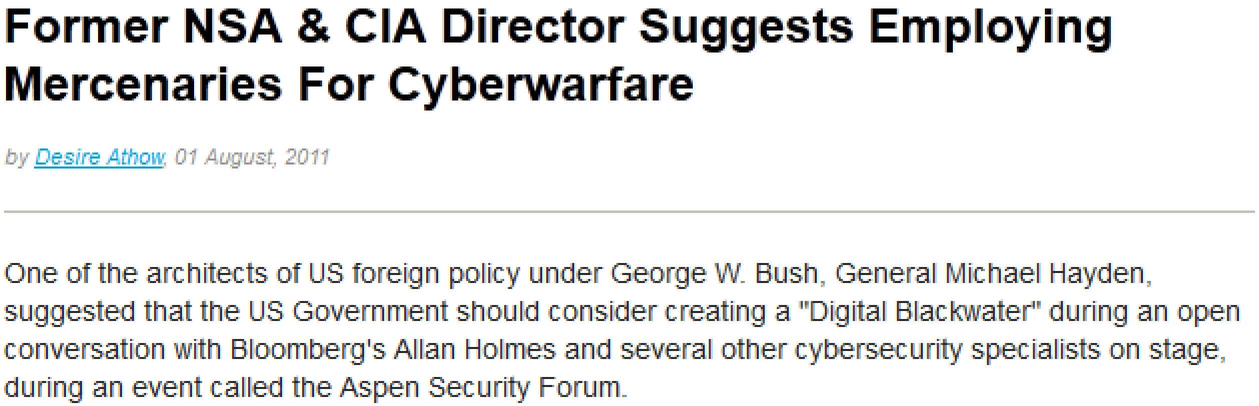
Retired Air Force Gen. Michael Hayden, formerly director of the Central Intelligence Agency and National Security Agency, is joining the security advisory firm The Chertoff Group as a principal, the firm announced today.



Former CNO Roughead Joins Northrop Grumman Board

(Press Release) Thursday, February 16

Northrop Grumman Corporation elected retired U.S. Navy Admiral Gary Roughead to its board of directors. Roughead served as the 29th Chief of Naval Operations for the Navy prior to his retirement from the service in 2011. The addition of Roughead increases Northrop Grumman's board of directors to 13 members, 12 of whom are nonemployee directors.



Former NSA & CIA Director Suggests Employing Mercenaries For Cyberwarfare

by Desire Athow, 01 August, 2011

One of the architects of US foreign policy under George W. Bush, General Michael Hayden, suggested that the US Government should consider creating a "Digital Blackwater" during an open conversation with Bloomberg's Allan Holmes and several other cybersecurity specialists on stage, during an event called the Aspen Security Forum.

- And if that wasn’t enough…
  - Boeing Integrated Defense Systems
  - Lockheed Martin Corporation
  - ManTech International
  - KEYW Corporation
  - Palantir Technologies
  - Science Applications International Corporation (SAIC)
  - Northrop Grumman Corporation
  - Raytheon Company
  - General Dynamics
  - NEK Cyber Operations Group
  - Thales Group
  - BAE Systems
  - Finnmeccanica
  - **And on and on and on…**

→ Privatization of «cyber-*»

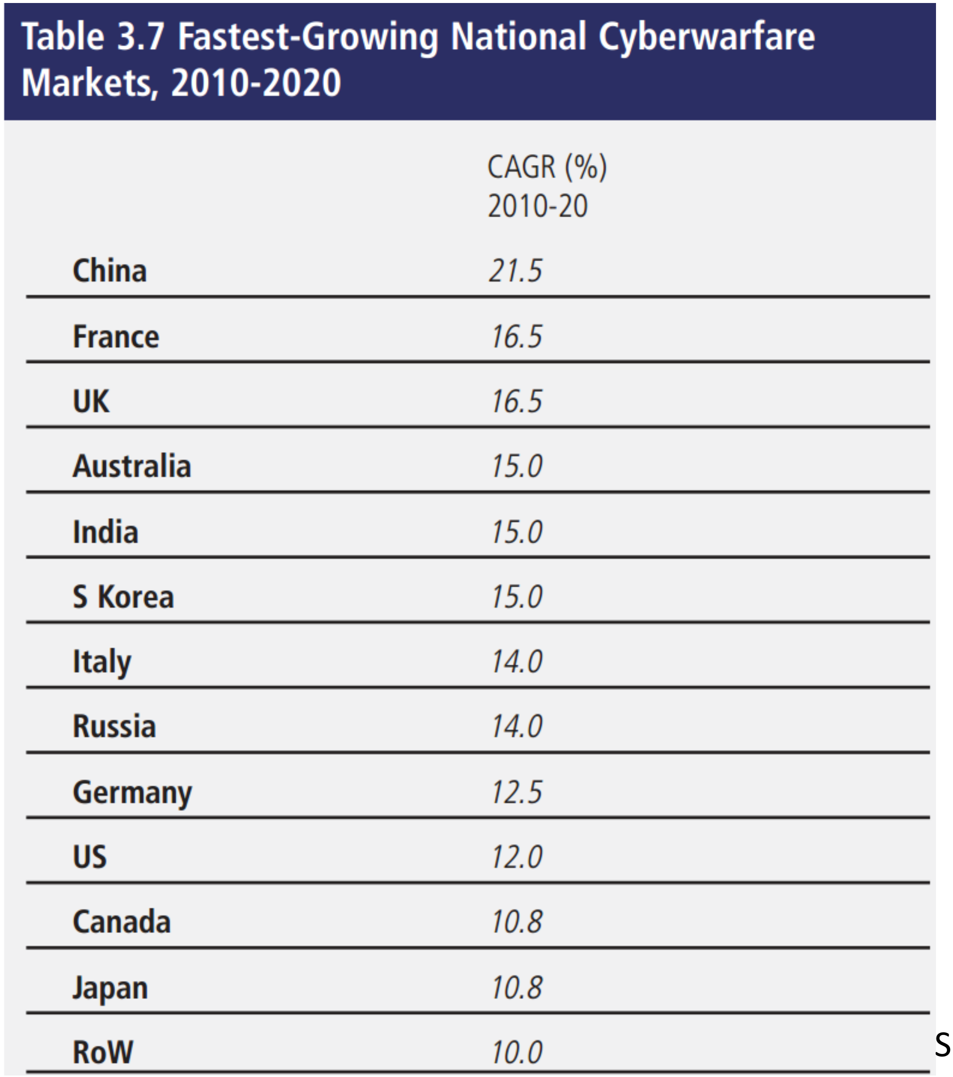
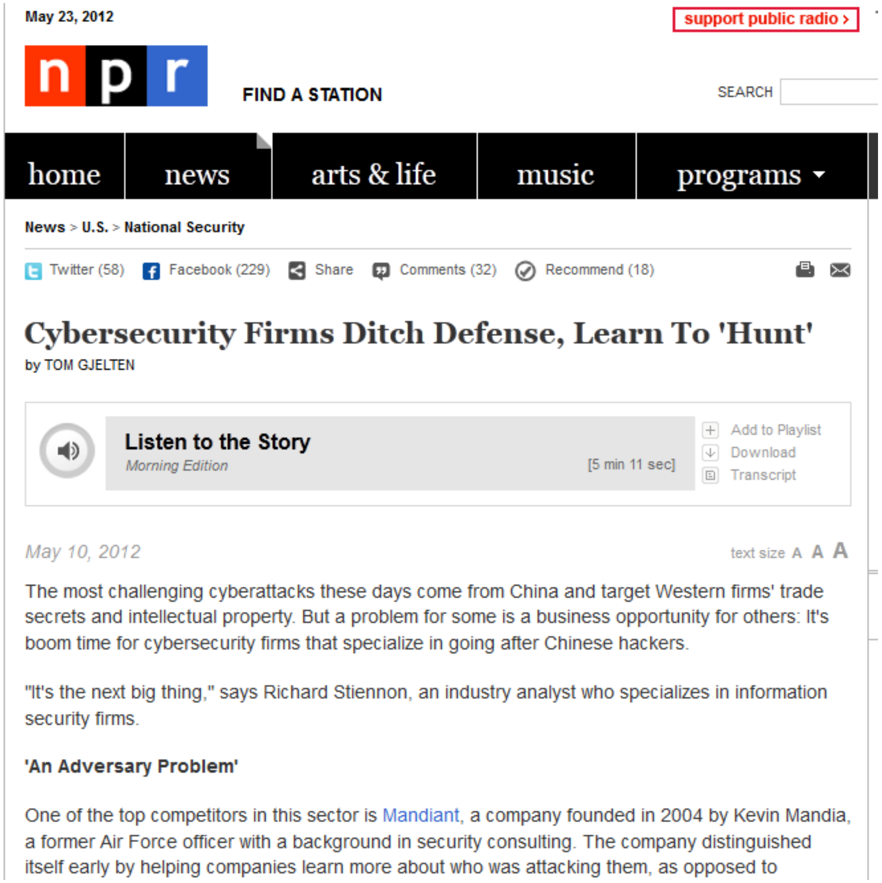


Table 3.7 Fastest-Growing National Cyberwarfare Markets, 2010-2020

	CAGR (%) 2010-20
China	*21.5*
France	*16.5*
UK	*16.5*
Australia	*15.0*
India	*15.0*
S Korea	*15.0*
Italy	*14.0*
Russia	*14.0*
Germany	*12.5*
US	*12.0*
Canada	*10.8*
Japan	*10.8*
RoW	*10.0*



May 23, 2012

News > U.S. > National Security

Cybersecurity Firms Ditch Defense, Learn To 'Hunt'

by TOM GJELTEN

May 10, 2012

The most challenging cyberattacks these days come from China and target Western firms' trade secrets and intellectual property. But a problem for some is a business opportunity for others: It's boom time for cybersecurity firms that specialize in going after Chinese hackers.

"It's the next big thing," says Richard Stiennon, an industry analyst who specializes in information security firms.

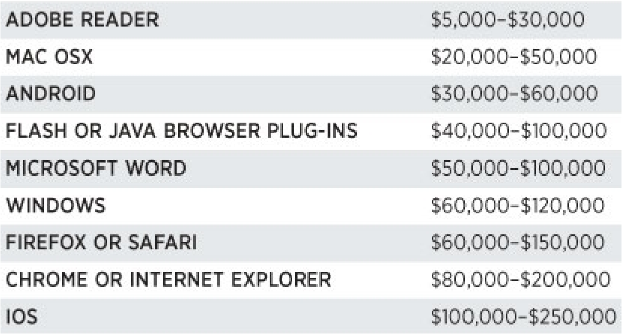
'An Adversary Problem'

One of the top competitors in this sector is Mandiant, a company founded in 2004 by Kevin Mandia, a former Air Force officer with a background in security consulting. The company distinguished itself early by helping companies learn more about who was attacking them, as opposed to

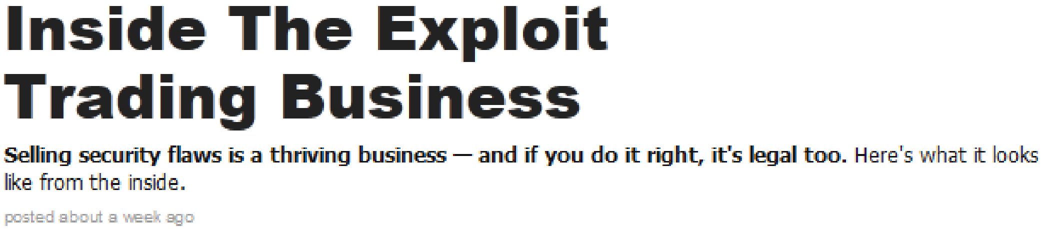
Source: *Cyberwarfare Market 2010-2020* by Visiongain

→ Privatization of «cyber-*»: CLOSER TO HOME

- While it **remains mostly unspoken**, European **intelligence agencies** also interface with the "security underground" **in their pursuit** for actionable intelligence, undisclosed vulnerabilities or tactical know-how.
  - While they don't have the same degree of control or coordination over their "contractors" as in certain other more centralized countries to the East, the **relationships are generally congenial and profitable for both parties**.
- If you don’t believe me, at least believe that they rely on the underground for logistical support:



ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000



Inside The Exploit Trading Business

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

posted about a week ago

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

Source: Forbes, “Shopping For Zero-Days: A Price List For Hackers’ Secret Software Exploits”, 2012, in http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

→ Privatization of «cyber-*»; exploits' market/1

Public Knowledge of the vulnerability	Buyer's typology
	
	IS = IT Security companies
	INT = Intelligence Agencies for Governmental use (National Security protection)
	MIL = MoD/related actors for warfare use
	OC = Cybercrime
		0-day Exploit code + PoC Cost: Min/Max

Y	IS	10K – 50K USD
Y	INT	30K – 150K USD
Y	MIL	50K – 200K USD
Y	OC	5K – 80K USD
N	ALL	x2 – x10

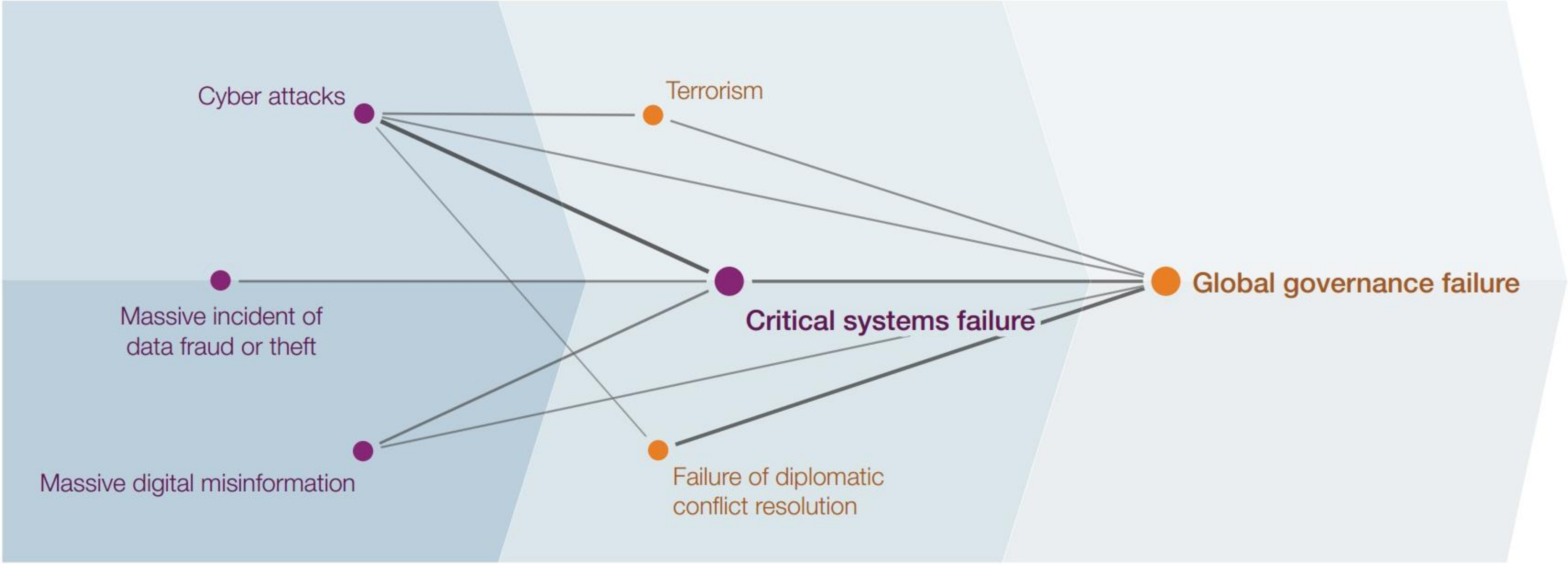
→ Privatization of «cyber-*»; exploits' market/2

Attribution or Obsfuscation of the Attack(s)	Vulnerability relays on: Operating System (OS) Major General Applications (MGA) SCADA-Industrial Automation (SCADA)	Buyer's typology ~~IS = IT Security companies~~ INT = Intelligence Agencies for Governmental use (National Security protection) MIL = MoD/related actors for warfare use OP = Outsourced «Partners» ~~OC = Cybercrime~~	0-day Exploit code + PoC : Min/Max
Y	OS	OP	40K – 100K
Y	MGA	INT	100K – 300K
Y	SCADA	MIL	100K – 300K
N	OS	OP / MIL	300K – 600K
N	SCADA	OP / MIL	400K – 1M

Outsourced to (Black) OPs

→ WEF Report 2012

Figure 17: The Dark Side of Connectivity Constellation


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

Origin Risk
Increasing capabilities for cyber crime and attacks.

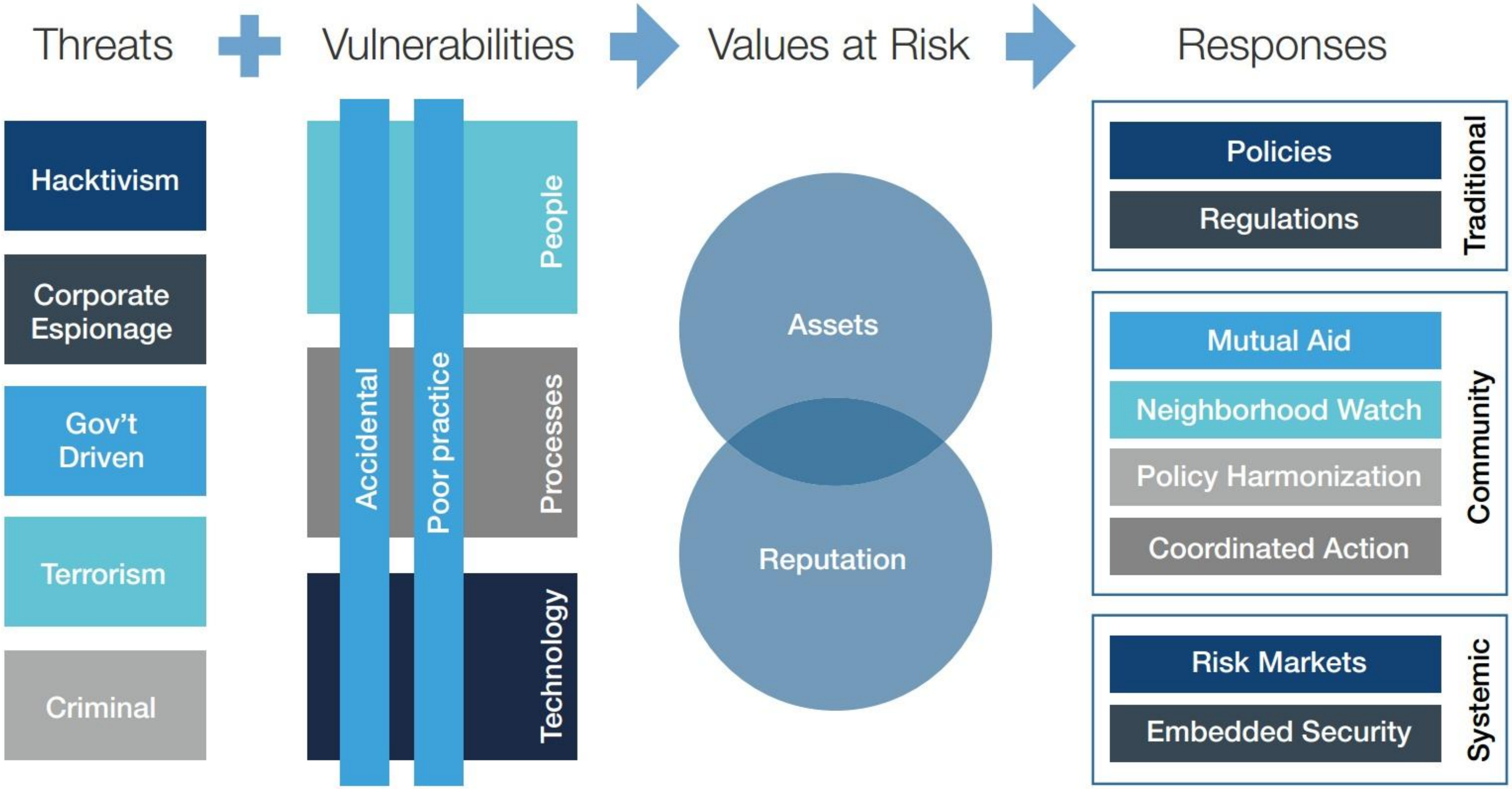
Pathways
Balance-of-power tips as new actors can wage effective interference and disrupt commerce.

Manifestation
The traditional system of global governance is undermined.

Source: World Economic Forum

→ WEF Report 2012

Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum

Building your own Cyber Army

→ Receipt «ByoCA» Rel. 1.0 aka «Build your own Cyber Army»

I. Understand, Identify, List, and Own your **weapons**.
  I. *Focus on goals and constrictions. Rules of engagement?*

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

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

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

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

VI. **Think** about new scenarios.
  I. *While hunting for old stuff…*

LA POLENTA

Ha il colore del sole, il sapore delle cose sane, il profumo della vita semplice. E' accolta con entusiasmo dai grandi e dai piccini e salutata trionfalmente anche dalle tavole più raffinate.

POLENTA DI FARINA GIALLA

Ingredienti: 250 gr. di farina gialla; 1 l. di acqua; sale quanto basta. - Perchè la polenta riesca buona, versare la farina occorrente nell'acqua bollente e salata, a pioggia, rimestando continuamente perchè la farina non faccia grumi. Sono indispensabili il fuoco vivo, il paiolo di rame e la cottura prolungata oltre i quaranta minuti. Quando è ben cotta, versare la polenta sull'apposito tagliere e tagliare con un coltello di legno o con uno spago.

POLENTA TARAGNA

Ingredienti: 250 gr. di farina di grano saraceno o farina nera; 1 l. di acqua; sale quanto basta; 250 gr. di burro; 250 gr. di formaggio magro e grasso. - E' la polenta squisitissima che si mangia in Valtellina, che è nutriente e saporita, che costituisce da sola il piatto principale del pranzo. Versare a pioggia la farina nell'acqua bollente, rimestando come per la polenta solita. A cottura quasi ultimata aggiungere il burro e il formaggio (ottimo il Bitto, il classico formaggio della Valtellina) tagliato a dadi, e servire fumante.

→ From Cybercrime to Cyber War

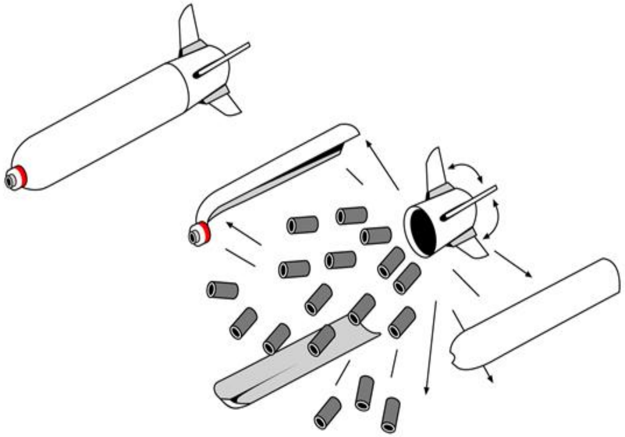
- Botnet & drone armies
- DDoS
- Trojans & Worms
- Malware
- Server hacking
- Encryption
- Extortion & Ransom
- Man in the Middle

Black Energy & alike

Stuxnet-like

- Cluster Bomb

- Cruise Missile



© 2009-2012 Jart Armin, Raoul Chiesa

→Cluster bomb VS Cruise

Black Energy

Multiple targets, loud and noisy

- Massive DDoS
- Loss of digital communication
- Cloning of state communications
- Create confusion

Stuxnet

Laser Guided, precision, and stealth

- Compromise infrastructure
- Industrial Sabotage
- Loss of confidence in systems
- Create confusion

- ❑ **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”.

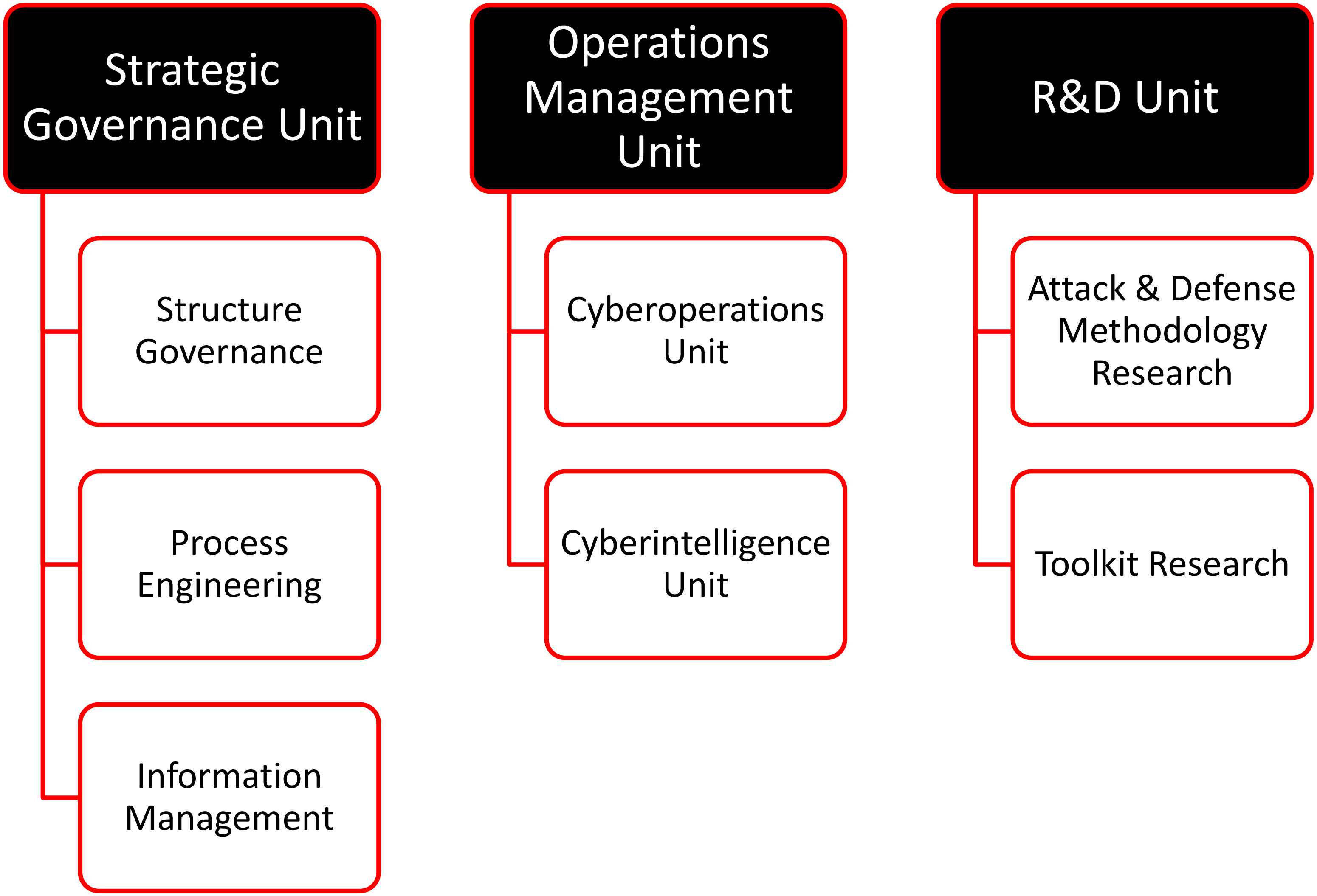
→ Offensive Security: recruiting

- ❑ Recruiting “digital soldier” within a State organization **is not feasible.**
- ❑ **Key and niche knowledge** of **experienced digital intelligence analysts** and **hackers** are required.
- ❑ Most attack technologies developed today **will became ineffective by 2 years** (max).

→ Cyber Warfare Unit (CWU)

- ❑ Concept to *quickly* and *effectively* **develop cyber offense capabilities.**
- ❑ **Partnership with private security industry** to establish “cyber war capabilities”.
- ❑ **Enhance** national and foreign **intelligence capabilities** in **cyberspace.**
- ❑ **Develop** cyber armaments and digital weapons for intelligence and military operations.

→ CWU: Organization



- Strategic Governance Unit
  - Structure Governance
  - Process Engineering
  - Information Management
- Operations Management Unit
  - Cyberoperations Unit
  - Cyberintelligence Unit
- R&D Unit
  - Attack & Defense Methodology Research
  - Toolkit Research

→CWU: Services

❑ Setup of organization units capable of:

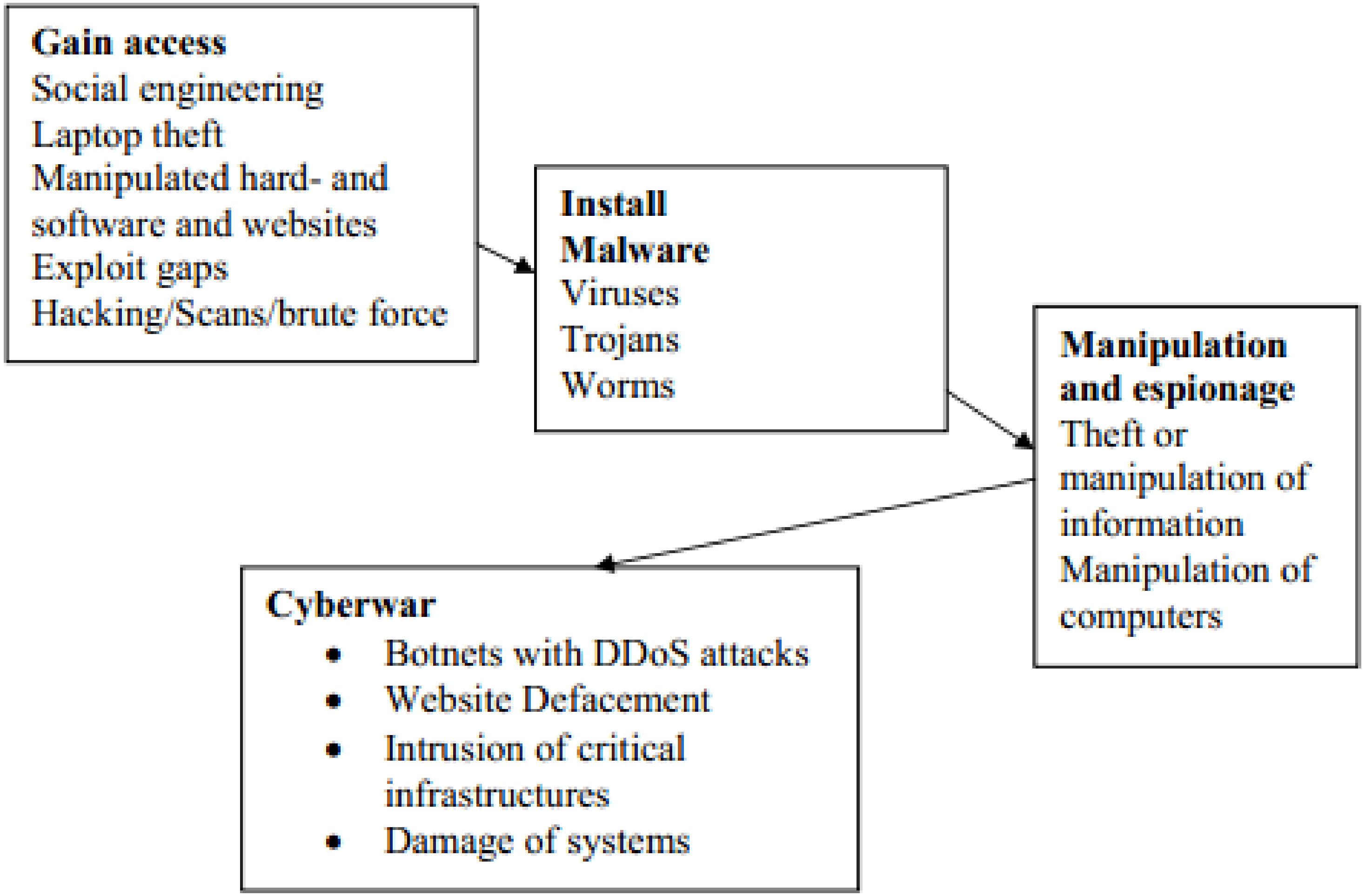
✓ **Supporting digital attacks** for intelligence operations in **civil** and **military** environments.

✓ **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**.

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



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

Install Malware
Viruses
Trojans
Worms

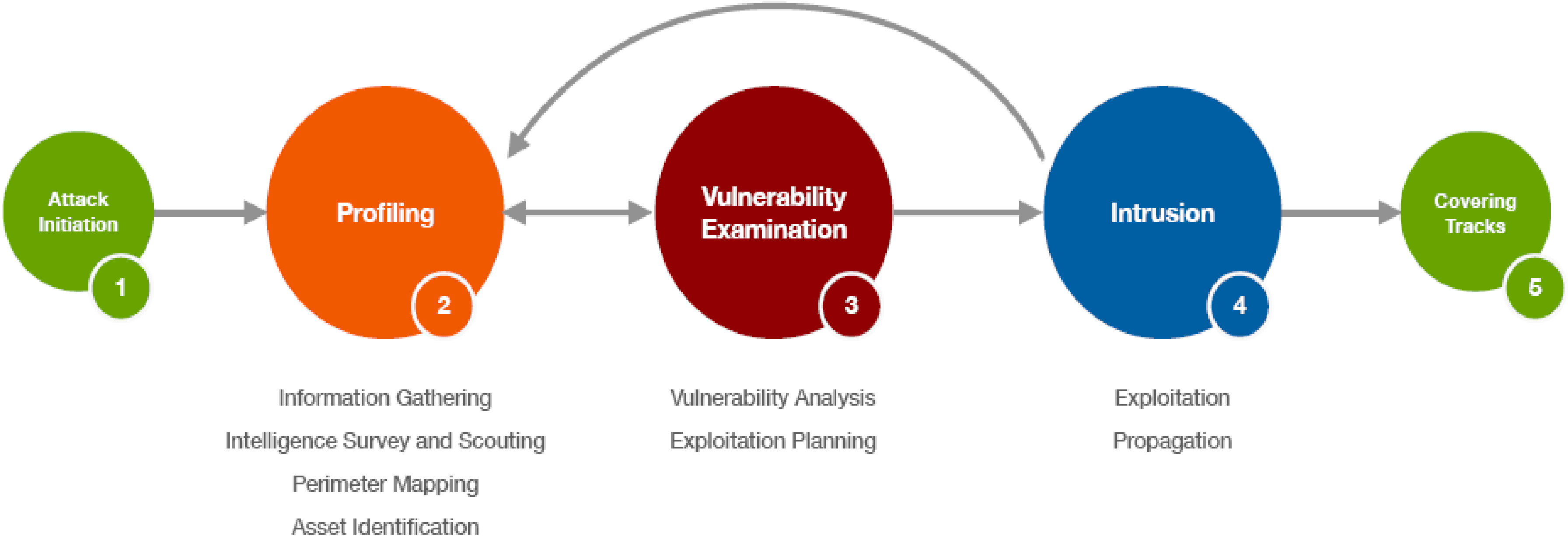
Manipulation and espionage
Theft or manipulation of information
Manipulation of computers

Cyberwar

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

Source: Saalbach, Cyberwar Methods & Practice

→ Cyber Attack «Methodology» (and, counter-attack), from an Hacker's Perspective



Source: Jim Geovedi, Indonesia

→ Actor attribution: does it matter?

„The greatest challenge is finding out who is actually launching the attack“.

Major General Keith B. Alexander,
Commander US CYBERCOM / NSA, testimony May 8th 2009,
„Cyberspace as a Warfighting Domain” – US Congress

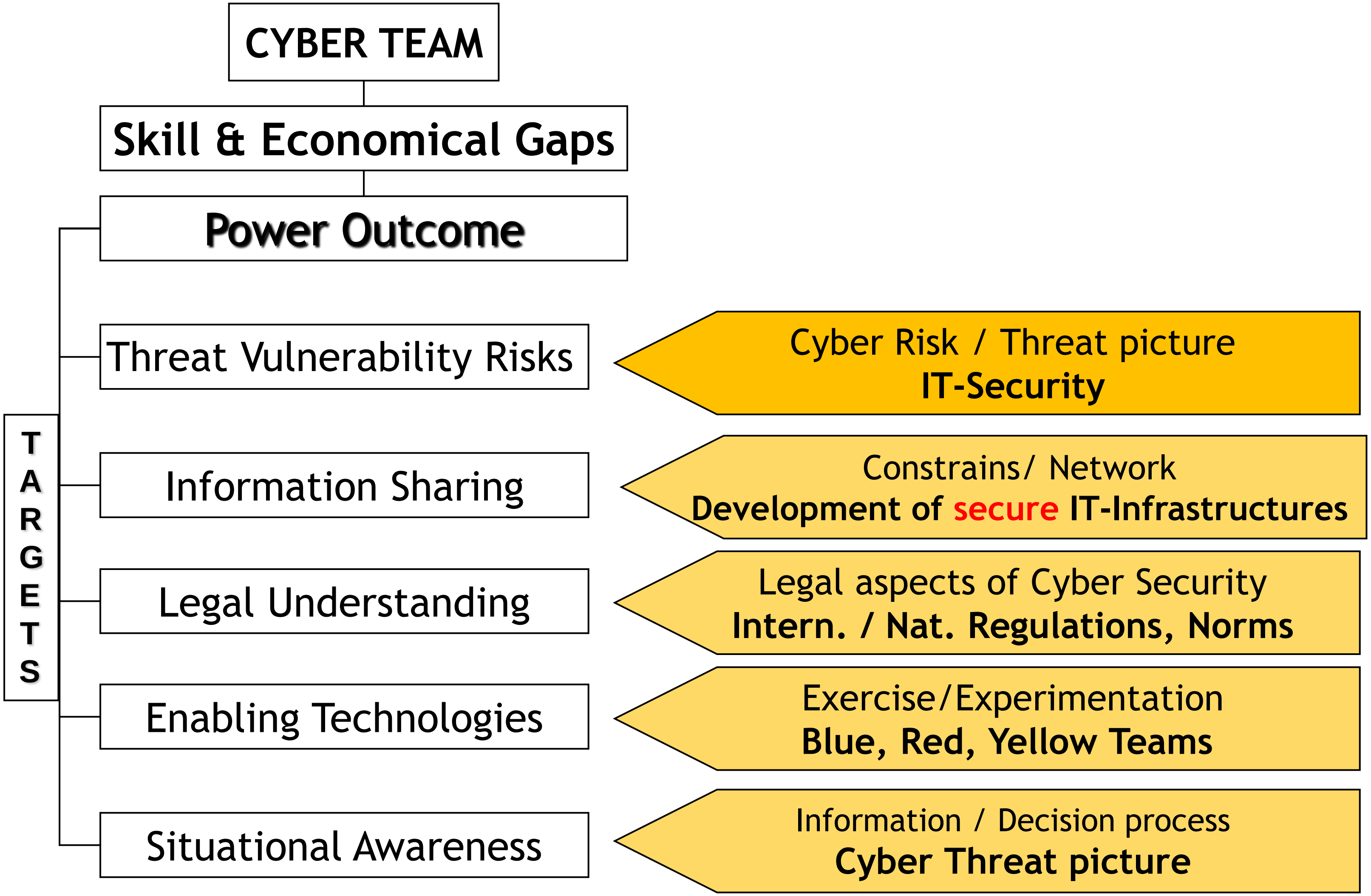
„Attribution is not really an issue“.
Senior DoD official, 2012 Aspen Strategy Group

Attribution:

tactical level = **irrelevant**
operational level = **helpful**
strategic level = **important**
political (board) level = **critical**

© Alexander Klimburg 2012

→ Setting up a proper team



CYBER TEAM

Skill & Economical Gaps

Power Outcome

TARGETS

Threat Vulnerability Risks

Cyber Risk / Threat picture
IT-Security

Information Sharing

Constrains/ Network
Development of secure IT-Infrastructures

Legal Understanding

Legal aspects of Cyber Security
Intern. / Nat. Regulations, Norms

Enabling Technologies

Exercise/Experimentation
Blue, Red, Yellow Teams

Situational Awareness

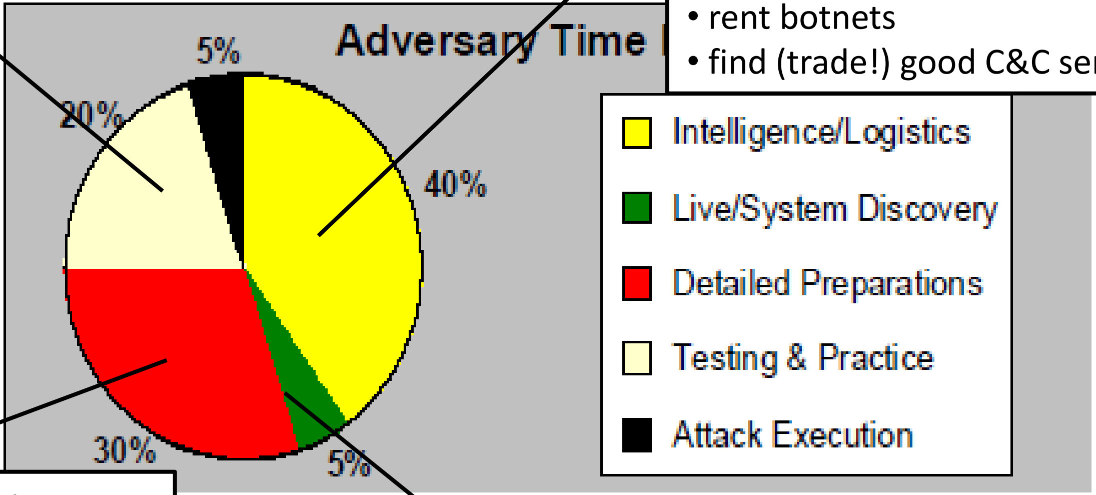
Information / Decision process
Cyber Threat picture

→ 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

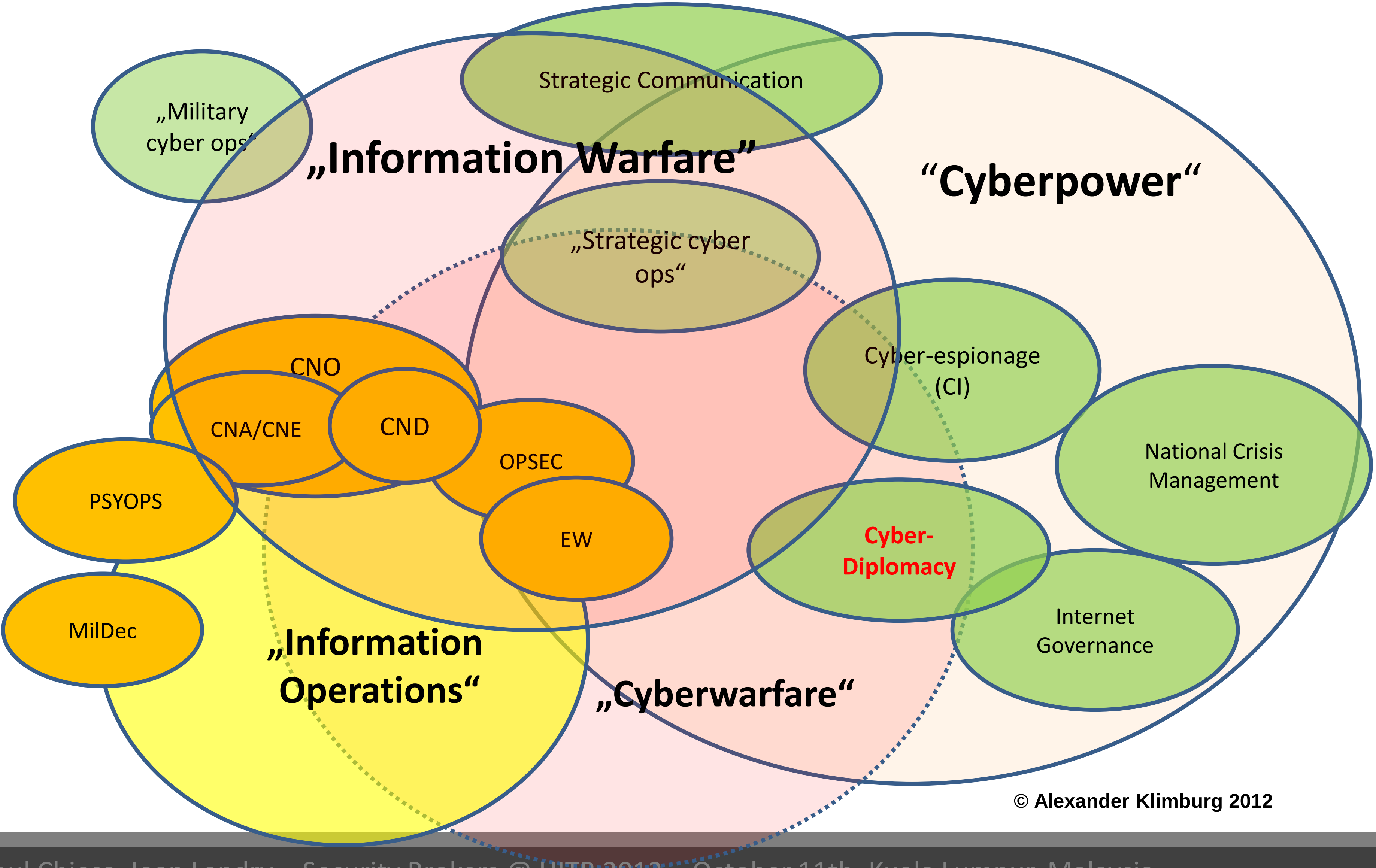


- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

•Purchase L2/L3 system data

© Alexander Klimburg 2012

→ It's outta there. Now.



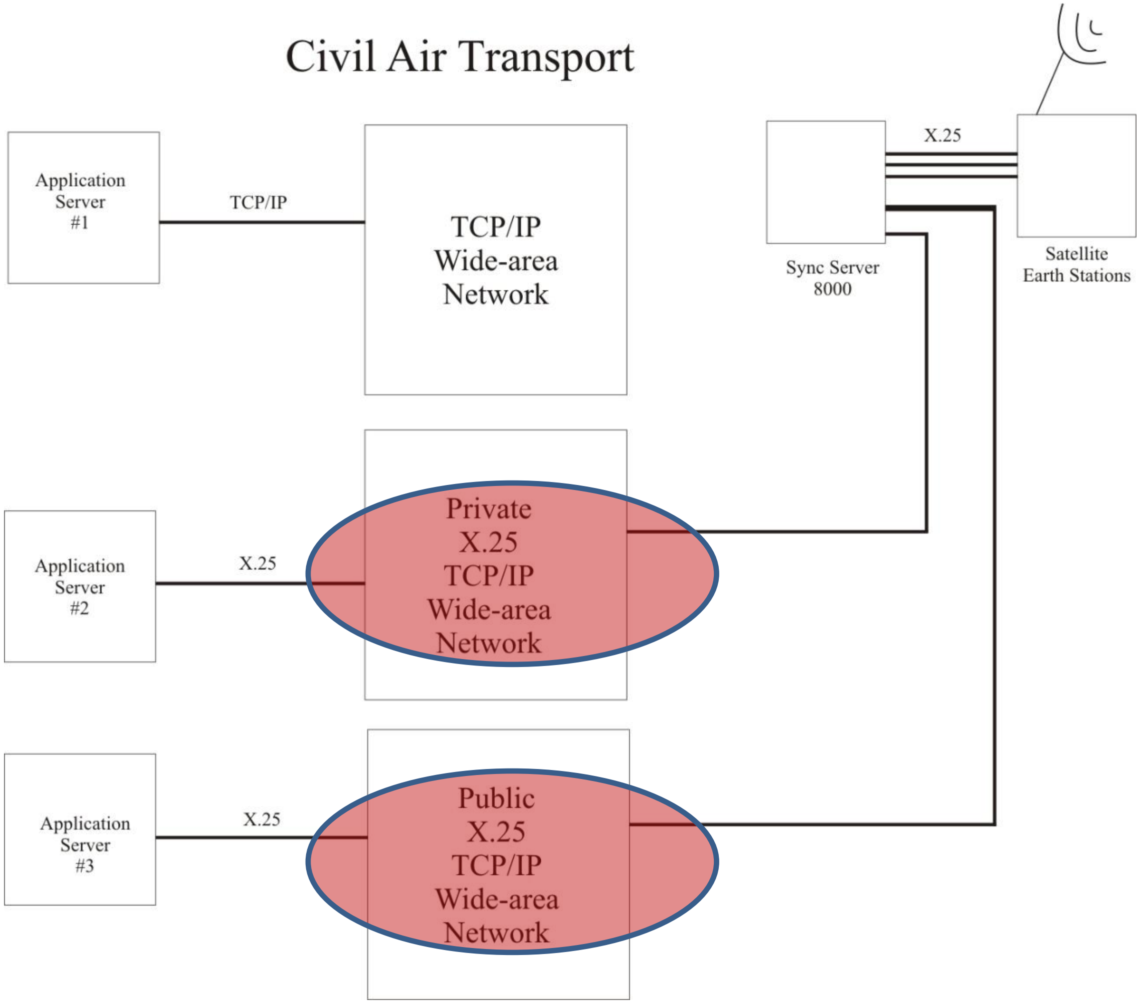
© Alexander Klimburg 2012

→ Cyberwar: a (theorical) case study

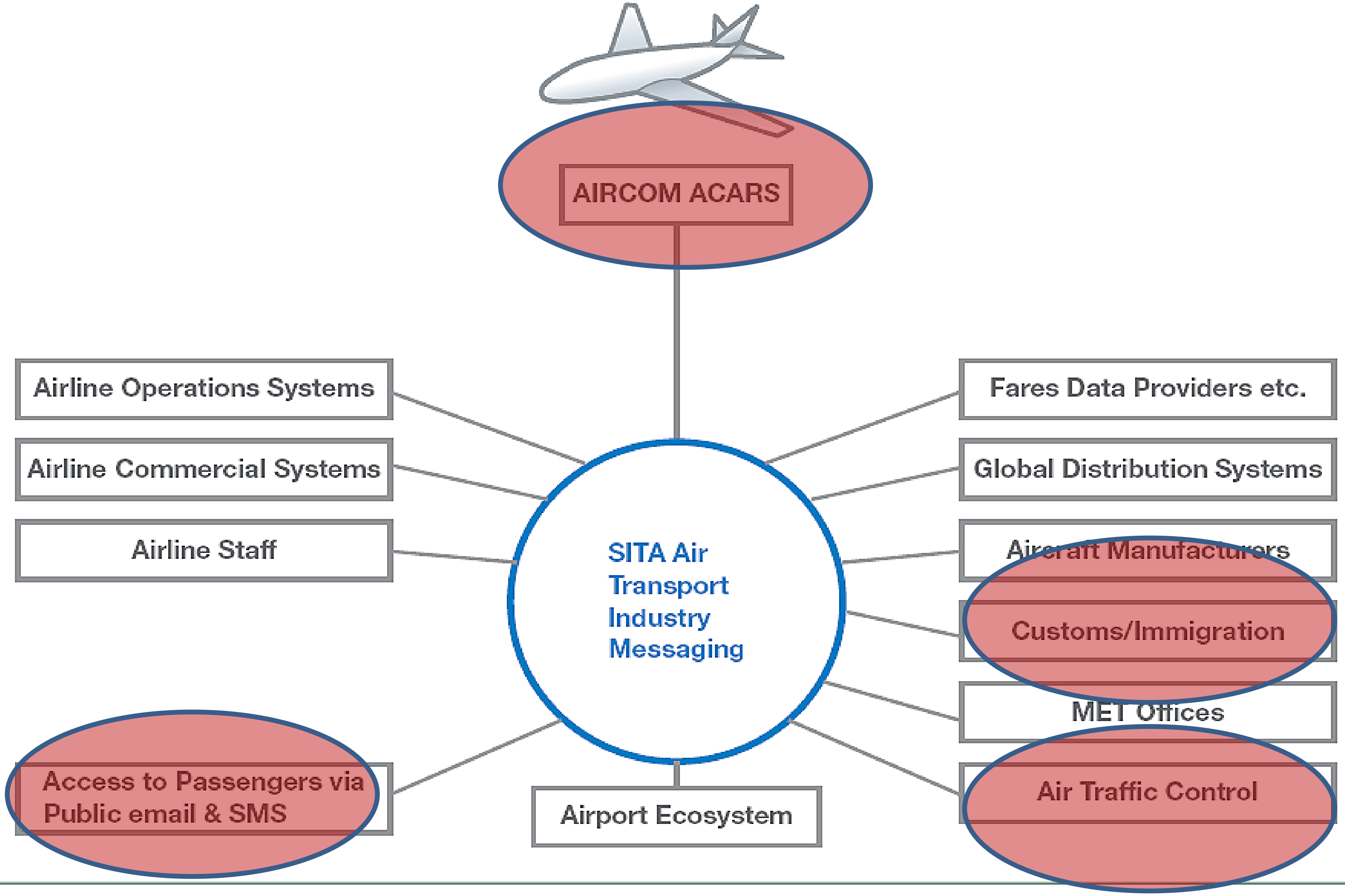
- Let’s get **creative**…
  - Ah, so many soft targets…
  - How about commercial aviation networks? They are often dual-purpose (useful from an intelligence perspective in peace-time, and relied on as logistical hubs in times of unrest or conflict).
  - In the latest time hackers are getting an increasing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

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

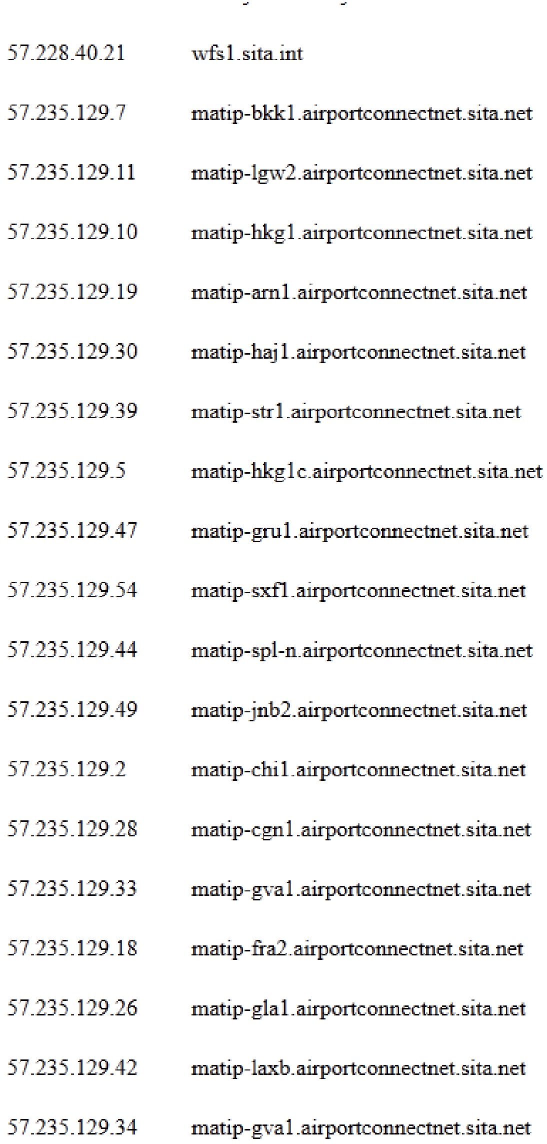
→ Cyberwar: a (theorical) case study



→ Cyberwar: a (theorical) case study


AIRCOM ACARS
Airline Operations Systems
Airline Commercial Systems
Airline Staff
Access to Passengers via Public email & SMS
SITA Air Transport Industry Messaging
Airport Ecosystem
Fares Data Providers etc.
Global Distribution Systems
Aircraft Manufacturers
Customs/Immigration
MET Offices
Air Traffic Control

→ Cyberwar: a (theorical) case study



57.228.40.21	wfs1.sita.int	
57.235.129.7	matip-bkk1.airportconnectnet.sita.net	
57.235.129.11	matip-lgw2.airportconnectnet.sita.net	
57.235.129.10	matip-hkg1.airportconnectnet.sita.net	Hong Kong International Airport
57.235.129.19	matip-arn1.airportconnectnet.sita.net	Stockholm-Arlanda Airport
57.235.129.30	matip-haj1.airportconnectnet.sita.net	
57.235.129.39	matip-str1.airportconnectnet.sita.net	
57.235.129.5	matip-hkg1c.airportconnectnet.sita.net	
57.235.129.47	matip-gru1.airportconnectnet.sita.net	
57.235.129.54	matip-sxf1.airportconnectnet.sita.net	
57.235.129.44	matip-spl-n.airportconnectnet.sita.net	
57.235.129.49	matip-jnb2.airportconnectnet.sita.net	
57.235.129.2	matip-chi1.airportconnectnet.sita.net	Chicago Airport
57.235.129.28	matip-cgn1.airportconnectnet.sita.net	Cologne Bonn Airport
57.235.129.33	matip-gva1.airportconnectnet.sita.net	Geneva International Airport
57.235.129.18	matip-fra2.airportconnectnet.sita.net	Frankfurt am Main Airport
57.235.129.26	matip-gla1.airportconnectnet.sita.net	
57.235.129.42	matip-laxb.airportconnectnet.sita.net	
57.235.129.34	matip-gva1.airportconnectnet.sita.net	

How much tonnage of cargo goes through Frankfurt every day?

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

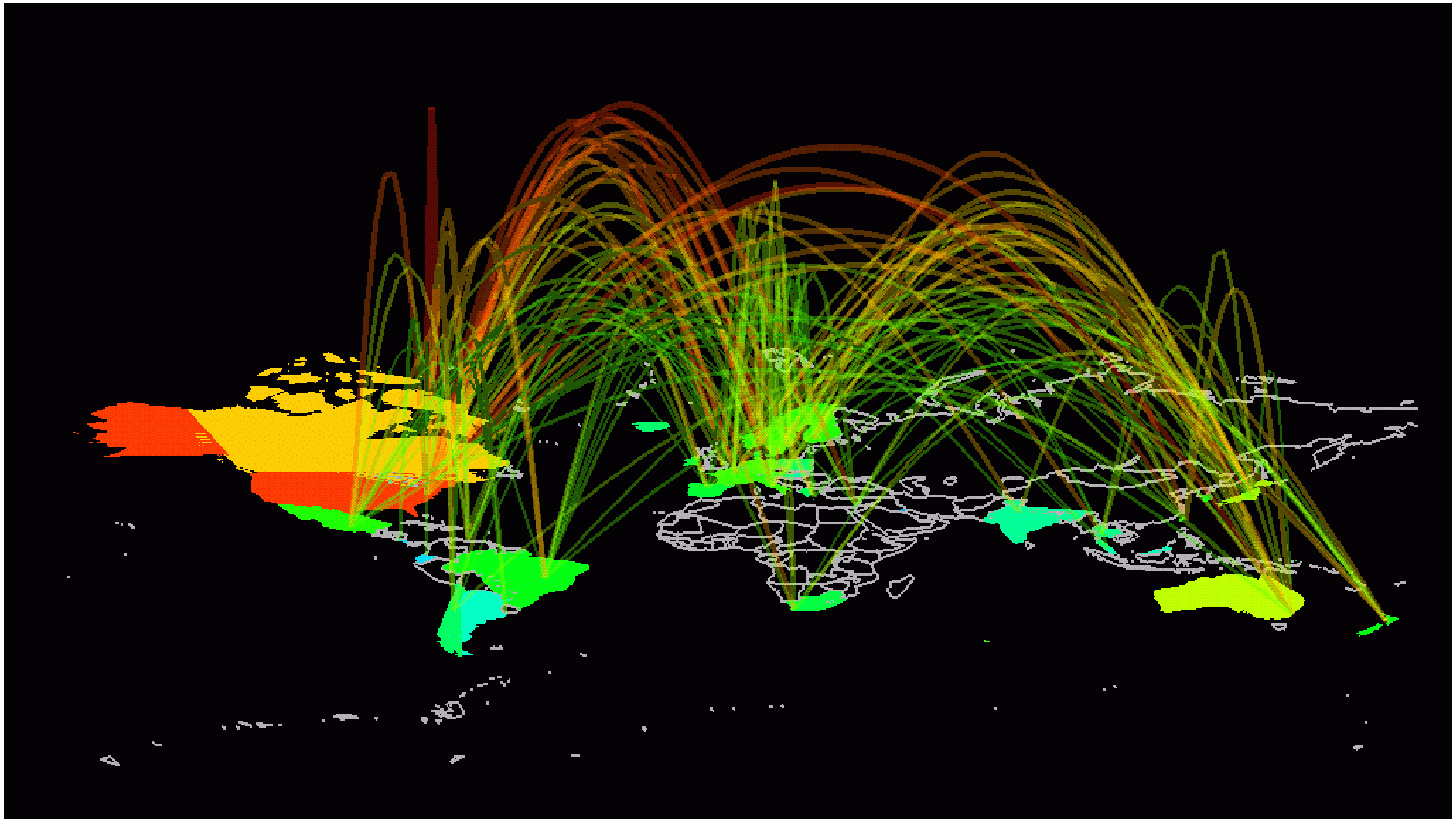
How much value is lost? Not a bad ROI for a 100k-500k USD investment...
Even keeping in mind that the goal is constant interruption (not destruction) of a supply chain and major economic hub.

→ **Summing up…**

- Cyber-Attacks **can be used to fit a goal**; and in **preparation to, during, and after a war**. But **wars cannot be won only by that**. The decisive battle will be still fought with regular forces.
- **Nations with high dependence on IT** are **in need of a central body** that **collects, analyzes,** and **assesses all pertinent information** from **government agencies** as well as **from private parties.**
- **No warning - surprising!**
- **Relative means** (compared to conventional attacks) = **great impact!**
- **Immediate effect worldwide!**

Traditional Force/Time/Space assessment
is not working anymore

→ Summing up…



Defenders have to protect against all possible channels of attack.

The **attackers** only have to **find one weak point** **to attack**

at a **time** and **place of their choice**.

→ Blue teams: what can YOU do?

- Most organizations buy a security suite, perform some quarterly or annual tests and assume they have continuous and flexible monitoring in place, while in reality they improved their security posture **from "entirely blind" to "mostly blind"**.
  - **So how do you defend against "state-serving adversaries", "APT" or otherwise very motivated adversaries?**
- Step 1: **ASSUME COMPROMISE**.
  - Cynical but critical.
- Step 2: **Develop** robust "threat awareness" or (if applicable) **CI procedures**.
  - "Cyberweapons" and accompanying methodologies are highly fungible and rendered obsolete once disclosed.
  - Added value: techniques and methodologies are often re-used for multiple campaigns by the same actors; analyzing the modus operandi can help in attribution over the long term.
- Step 3: **Exchange intelligence** with your peers, even internationally.
  - Examples: threat intelligence, indicators of compromise & signatures, disclosure of data breaches.

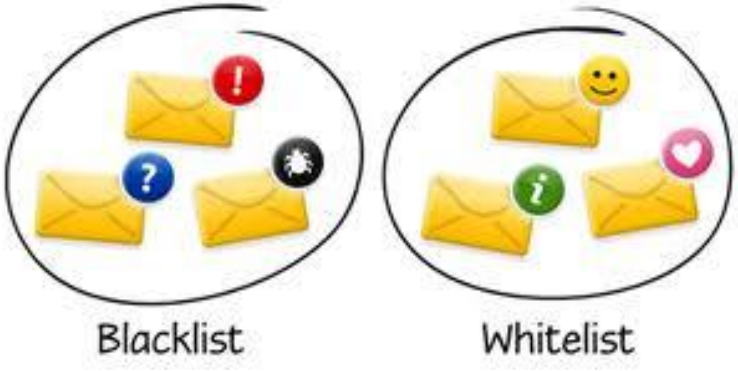
→ **We know this.**

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

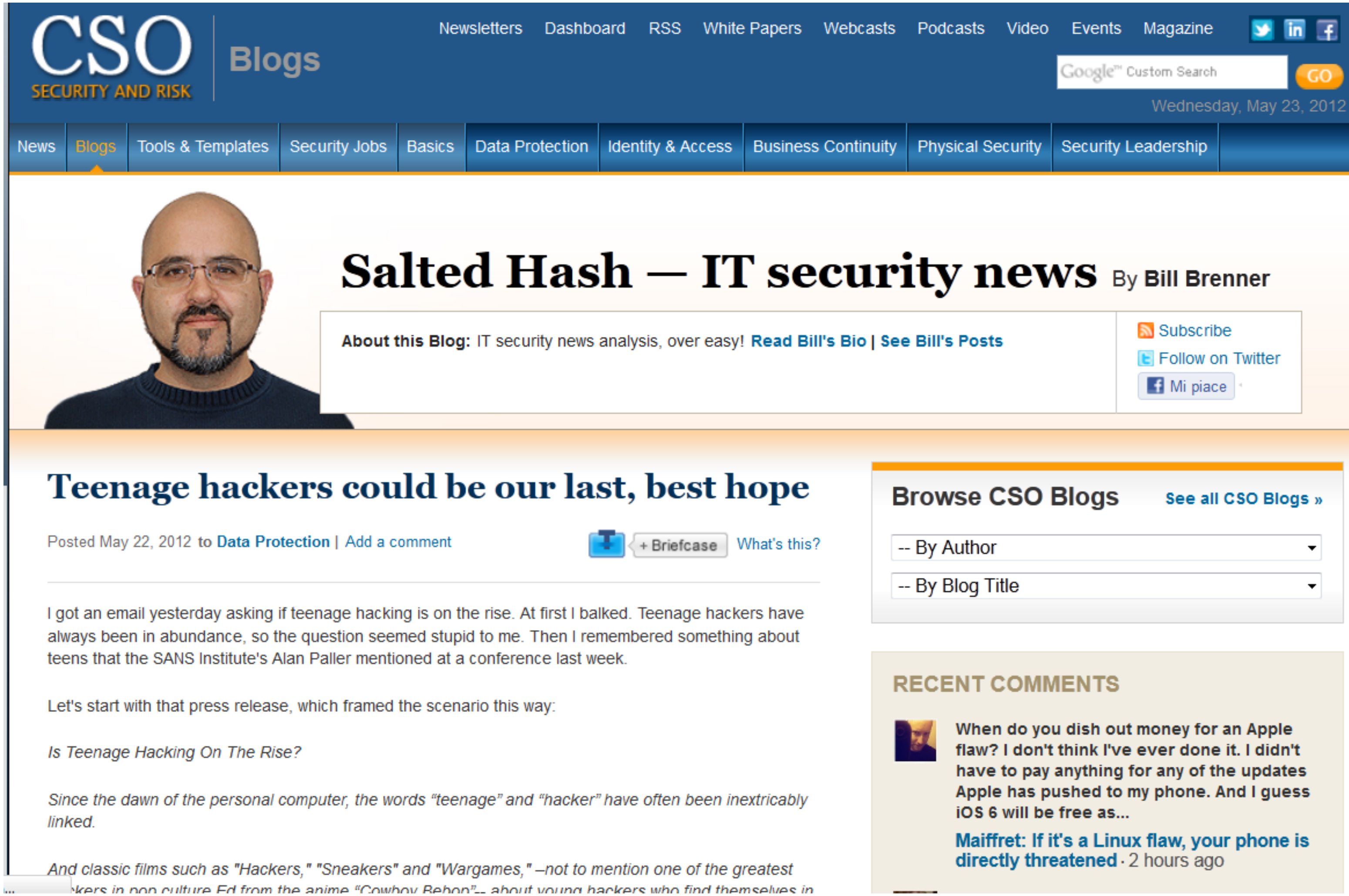
- ✓ Find a **victim** who should «coordinate» them («the g», LOL!!)
- ✓ Identify the **Team Leader** (seriously)
- ✓ **Get your** «Man at the Havana» (w/ Robert Redford's style)
- ✓ Run a **market survey** (yup…there ARE competitors!!)
    - ❖ +120 countries are developing Cyber Warfare capabilities: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

→ But…there's always a BUT!

- **Pay attention**: it's a «very weird market» that is **easily disturbed**.
    - As in, an aquarium is easily disturbed by ***introduction of a new fish*** or ***outside disturbance*** ☺
- **Be clear**, be «fair»: set up **rules, respect them**.
- **It's not a game**.
- **Actors** involved may **betray you** (from all around…)
- Stay in the **white-list**.



Thinking AHEAD!



Salted Hash — IT security news By Bill Brenner

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

Teenage hackers could be our last, best hope

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

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

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

Is Teenage Hacking On The Rise?

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

And classic films such as "Hackers," "Sneakers" and "Wargames," –not to mention one of the greatest ...kers in pop culture Ed from the anime "Cowboy Bebop"-- about young hackers who find themselves in

Browse CSO Blogs

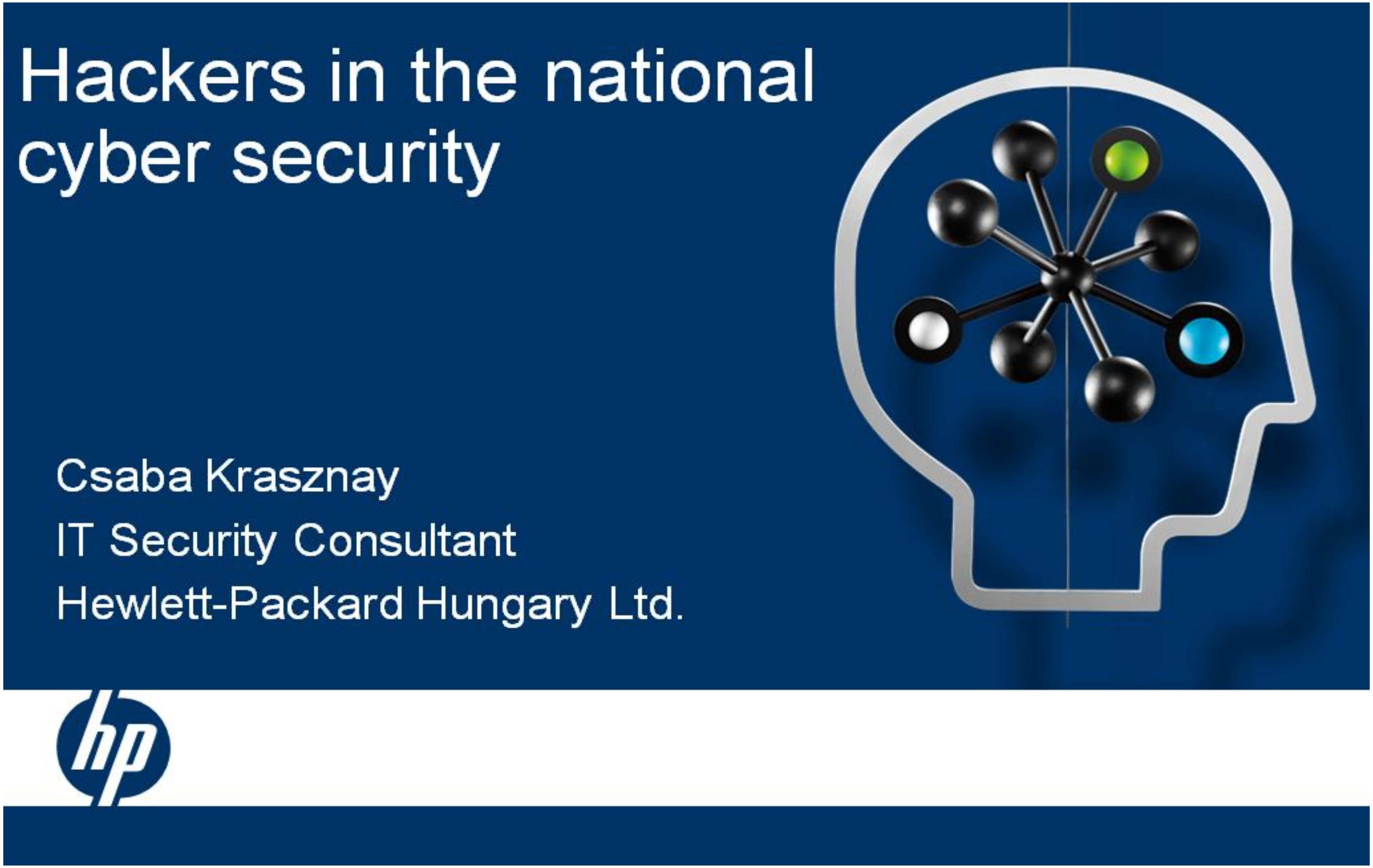
RECENT COMMENTS

When do you dish out money for an Apple flaw? I don't think I've ever done it. I didn't have to pay anything for any of the updates Apple has pushed to my phone. And I guess iOS 6 will be free as...

Maiffret: If it's a Linux flaw, your phone is directly threatened · 2 hours ago

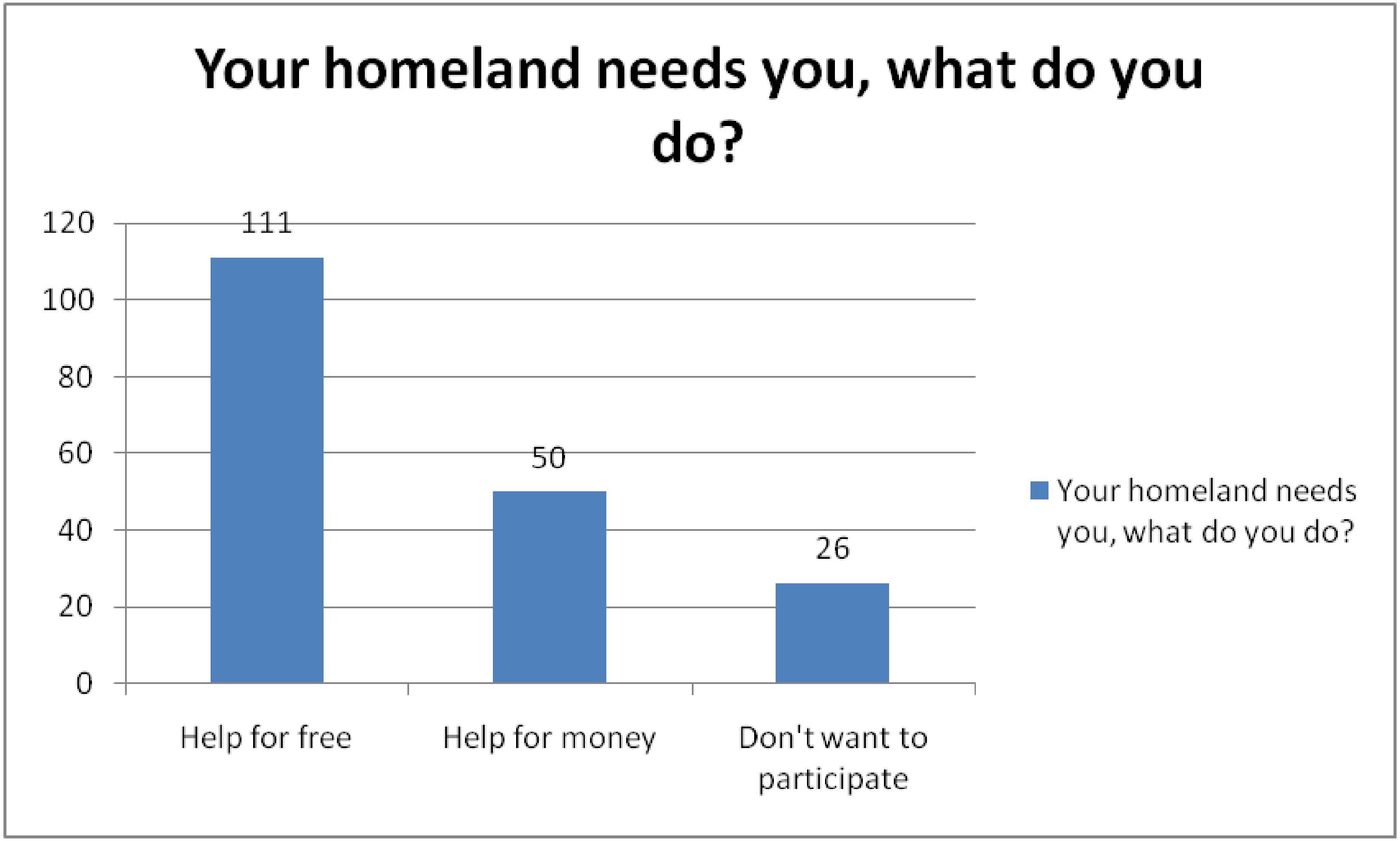
http://blogs.csoonline.com/data-protection/2193/teenage-hackers-could-be-our-last-best-hope

→ DIYO as a job



Hackers in the national cyber security

Csaba Krasznay
IT Security Consultant
Hewlett-Packard Hungary Ltd.



Source: “Hackers in the national cyber security”, Csaba Krasznay, HP: Hacktivity 2010, Hungary.

→ 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

Credits

❑ Kudos to:

✓ Ioan Landry

✓ Jart Armin

✓ Francesca Bosco

✓ Alexander Klimburg

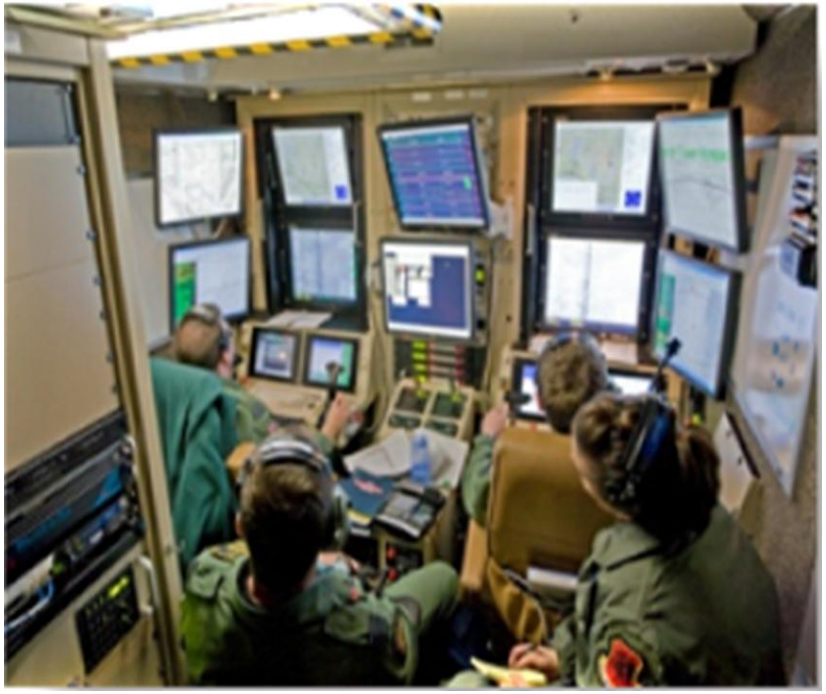
✓ Indianz.ch

✓ Naif

✓ «Cyber-Lawyer» Dr. Stefano Mele

✓ Colonel Josef Schroefl, Austria MoD

✓ Andrea Zapparoli Manzoni

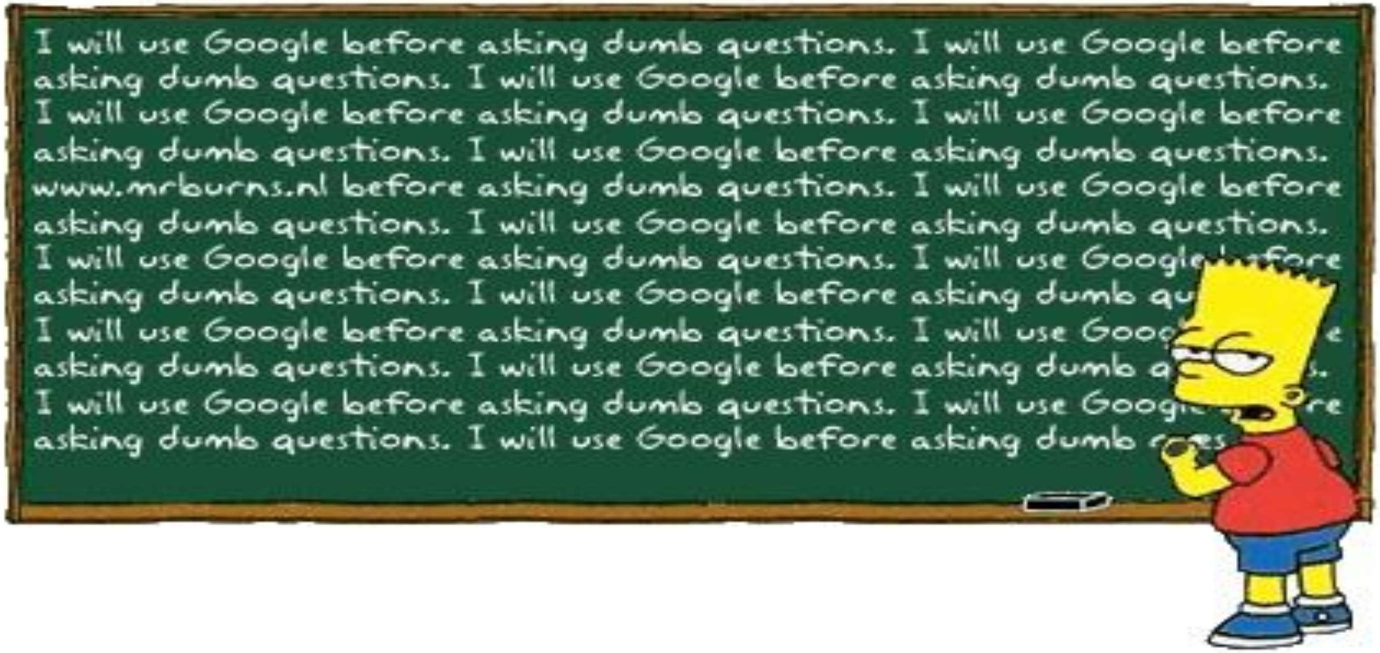


❑ Supporters:

✓ The HITB Crew

✓ Dhillon, Belinda, Amy ☺

→ 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 ques

SecurityBrokers
Global Cybersecurity Defense Services

Raoul «nobody» Chiesa

rc@security-brokers.com

SUBJ: HITB KUL 2012

GPG Key:
http://raoul.EU.org/RaoulChiesa.asc