PUBLIC RELEASE

Ladies and Gentlemen, here's *Your* Cyber Army!
(from a Hacker's perspective, of course :)
aka "Cyber Warfare 2.0"

PUBLIC RELEASE






Raoul «Nobody» Chiesa

Founder, Partner, **Security Brokers**

Principal, **CyberDefcon Ltd.**

SecurityBrokers
Global Cybersecurity Defense Services

CyberDefcon

This is the Agenda!

- Introductions
- Scenarios
  - The official one
  - The unofficial one
  - The real one
  - Definitions w/ a possible case study
- Nation's worldwide status
  - Hot Players
- Building your own Cyber Army
  - General model
  - Business model
  - Operating model
  - Costs analysis
  - Attack Operations….opsss! I mean «Offensive Behaviour! - Costs & Timeframes
- Conclusion
- Credits, Contacts, Q&A


Disclaimer
FEYENOORD

→Disclaimer

- Due to the **very sensitive nature of the topic**, it is **not permitted to take photographs or audio and/video recordings of this presentation**: please hold all photography **until Q&A**.
  - Of course, you may easily hide a mini-camera or park your smartphone on the desk while and filming: **you would lose my friendship though**.
  - Consider **what's more important** for you...
  - Also, please note that , the Key Note will be videorecorded by CONFIdence X staff, cleaned out of some frames, then it will be released.

- 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.

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


Introductions

Raoul Chiesa

- Founder, Partner, **Security Brokers** Inc.
- Principal, **CyberDefcon** UK
- Senior Advisor & Strategic Alliances on Cybercrime presso l'**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 Observtory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Founder, Owner, **@ Mediaservice.net**

Security Brokers

- Security Brokers (SB) was established after **three year-long phase** of «*human start-up*» and bootstrapping.

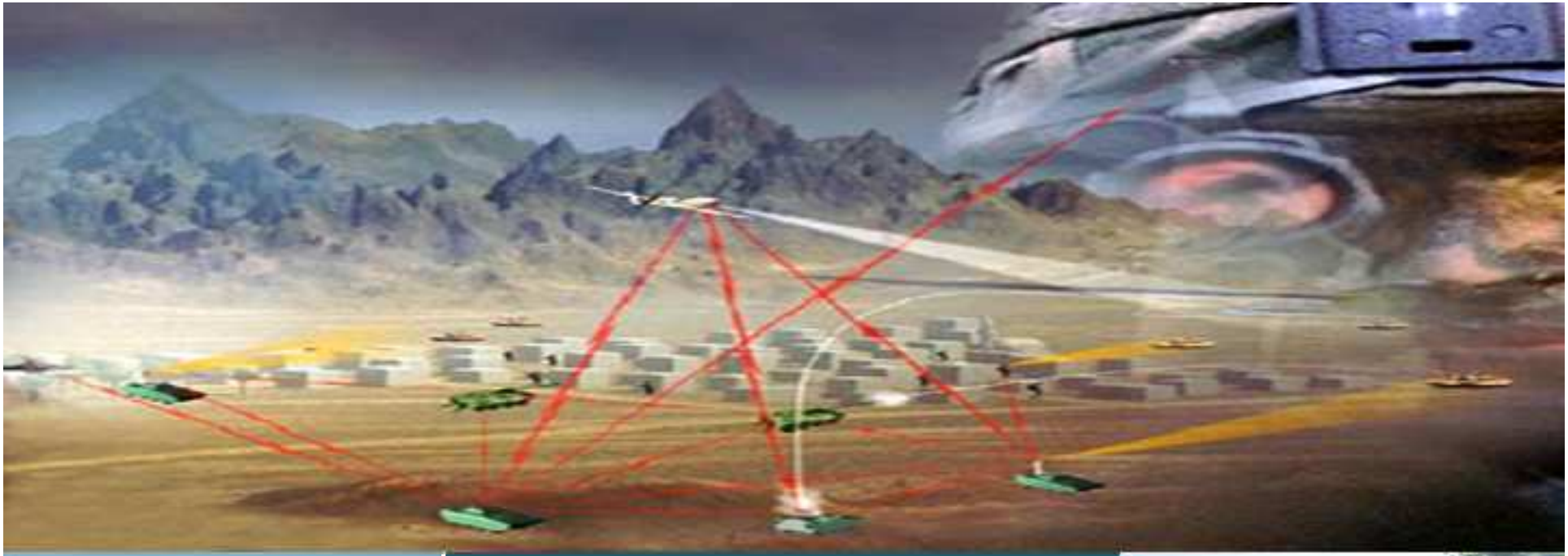
- SB's **concept** can be summarized as an agile **IT and InfoSec marketplace provider with 360° vision**, which uses a **business model similiar to traditional brokerages**: we locate the best «product» (expert, service, product), typically located in «niche» sectors to best serve our clients.

- The model itself is based chiefly upon **personal** relationships and networks cultivated over 20 years and tried & tested in the field over the past **10 years**.
- This said, SB has as «input» its own key **Suppliers** (Associates) and its **High-Level Independent Consulting Services** as «output».

- The full listing of SB's Associates **is not yet public** (ETA: JUL/SEPT 2012), though it encompass many respected Ethical Hackers, IT Security Researchers and top-class experts.

Security Brokers.

- We focus on critical and interesting topics. Thanks to the know-how and specialization our **30+ global experts** have gathered over **20 years of demonstrable field experience** in the **Information Security** and **Cyber Intelligence** communities (and a few others!), we can claim **over 600 combined references per year.**
- Our **main service areas** can be summarized here:
  - **Proactive Security**
    - With a focus on mobile networks and devices, modern telco networks, SCADA/NCI security, IA in the Transport, Space & Air sectors, social networks, and proactive identification and mitigation of security issues.
  - **Post-Incident & Incident Response**
    - Attacker profiling, Digital Forensics (Host, Network, Mobile, GPS, etc..), Training
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Psychological, Behavioural and Social aspects of hacking and infosec**
  - **Cybercrime**
    - Botnet takeovers and takedowns, Cybercriminal profiling and bounties, Cyber Intelligence reports, facilitator towards external CERTs and LEAs/LEOs, […]
  - **Information Warfare, Information Superiority & Cyber War** (intended exclusively for MoD clients)
    - 0day vulnerabilites and "digital munitions"; OSINT Trainings & Services; CNA/CND/CNE



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

SecurityBrokers
Global Cybersecurity Defense Services

«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, estimation: 6-12 BLN USD$/year

Source: Group IB Report 2011

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

SLIDE NOT PRESENT IN THE PUBLIC RELEASE OF THIS PRESENTATION
(YOU SHOULD HAVE ATTENDED CONFIDENCE X 2012!)

SLIDE NOT PRESENT IN THE PUBLIC RELEASE OF THIS PRESENTATION
(YOU SHOULD HAVE ATTENDED CONFIDENCE X 2012!)

→ Reasons for this talk/2: my experiences with «Info War»

- **1986-1995**: I hacked into most of the world's military and Government's environments and Data Networks (good old times! ;)
- **2009-2011**: Supporter of INTERPOL's & Team Cymru's folks
- **March-August 2010**: the "COPASIR REPORT": I've been Interviewed by the COPASIR (Italian Parlament Committee for the Security of the Republic), which then published the final report (public, in Italian).
- **June 2011**: Speaker at the ICCC (International Conference on Cyber Conflict) in Tallin, Estonia, for the CCDCoE (NATO Cooperative Cyber Defence Centre of Excellence).
- **September** 2011: Key Note Speaker at the GOV.CERT Poland Conference, Secure 2011 .
- **November 2011**: Speaker at the GOV.CERT of The Netherlands
- **May 2011**: Among the founders of the "CyberWorld" Working Group at the CASD (Center for Higher Defense Studies) inside the OSN (National Security Observatory) at the Italian Ministry of Defence.

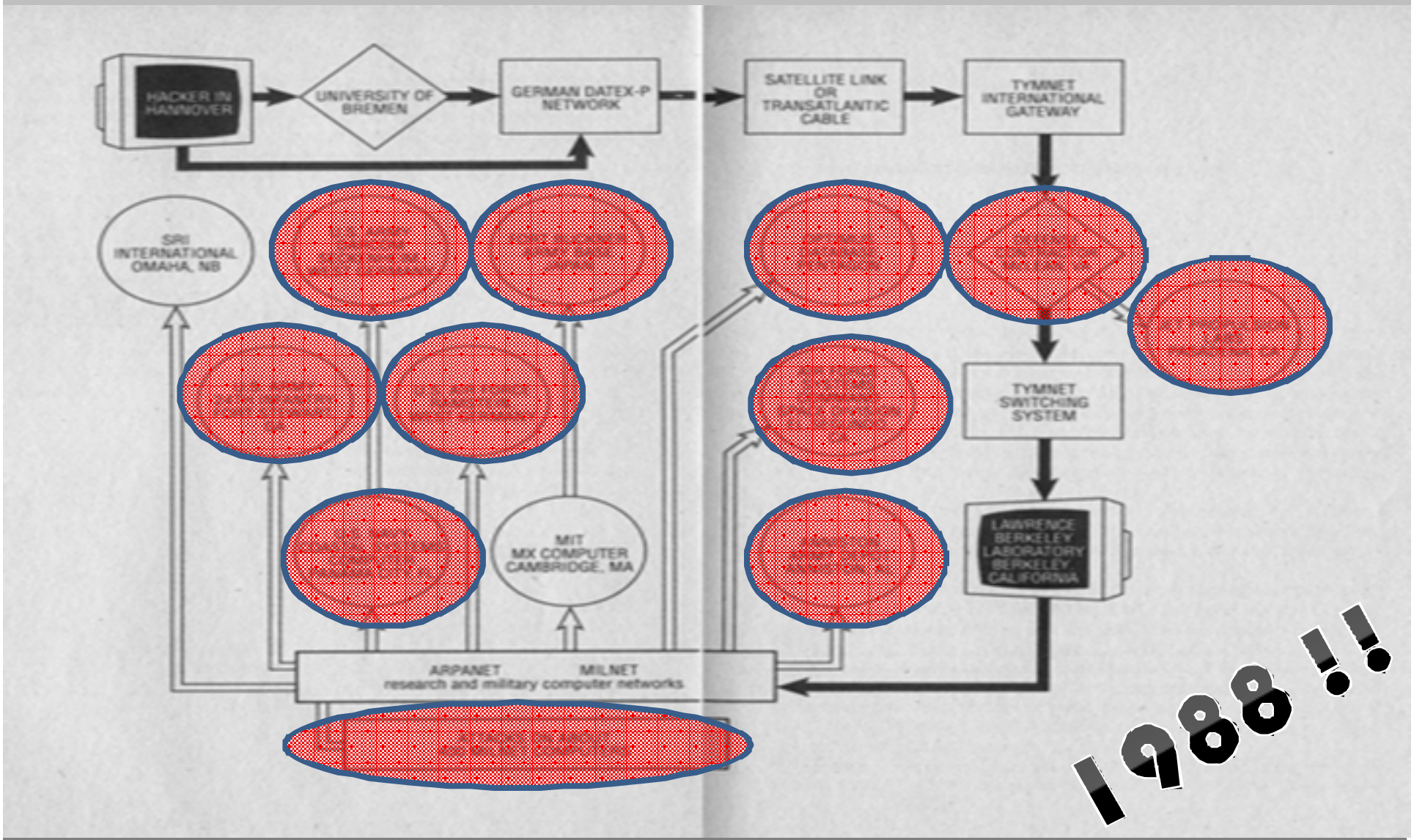
→ What happened 'till now?

Source: Andrea Zapparoli Manzoni, Security Brokers

→ Right? NO!!!

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

→ **Back to the 80's…**

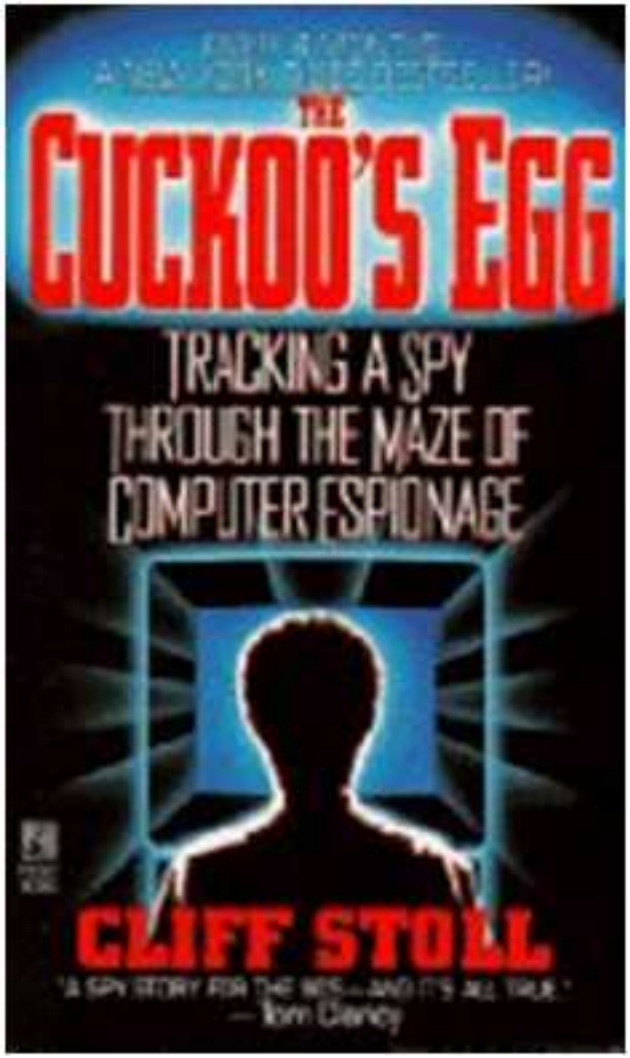


→ Back to the 80's...

- 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

- **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)

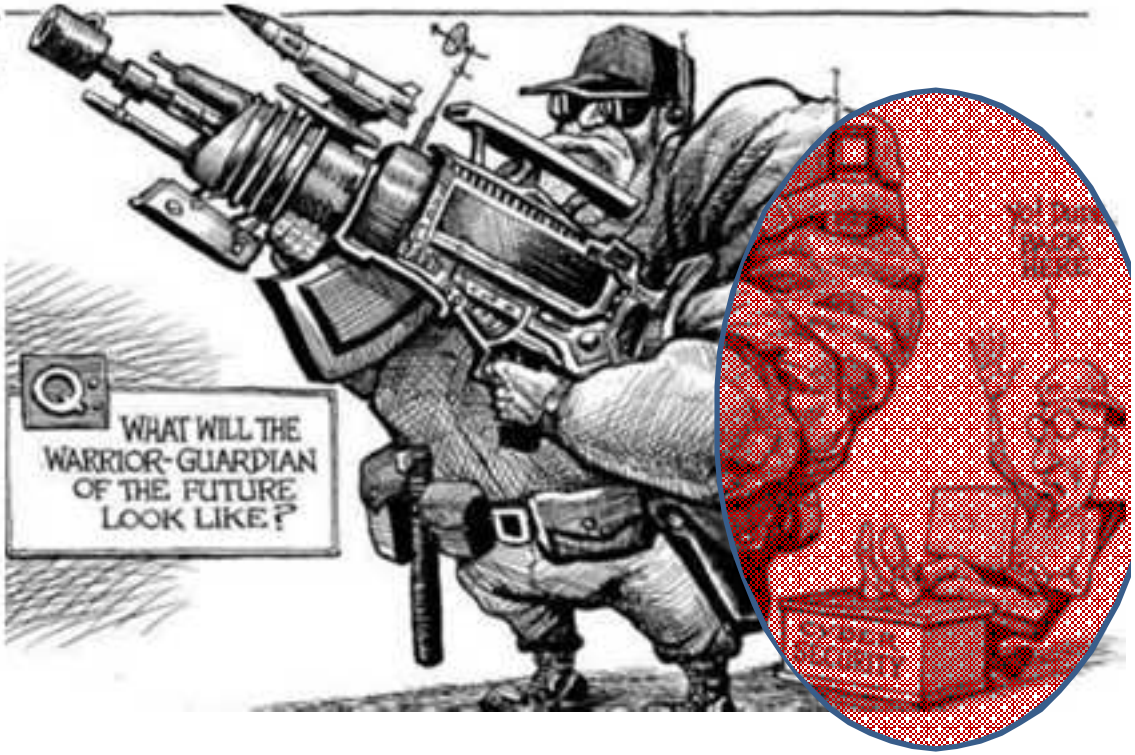
The Way-Future machine

"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 2012? ☺ LOL!!



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

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-Criminal	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 – 2011-2012)

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)**

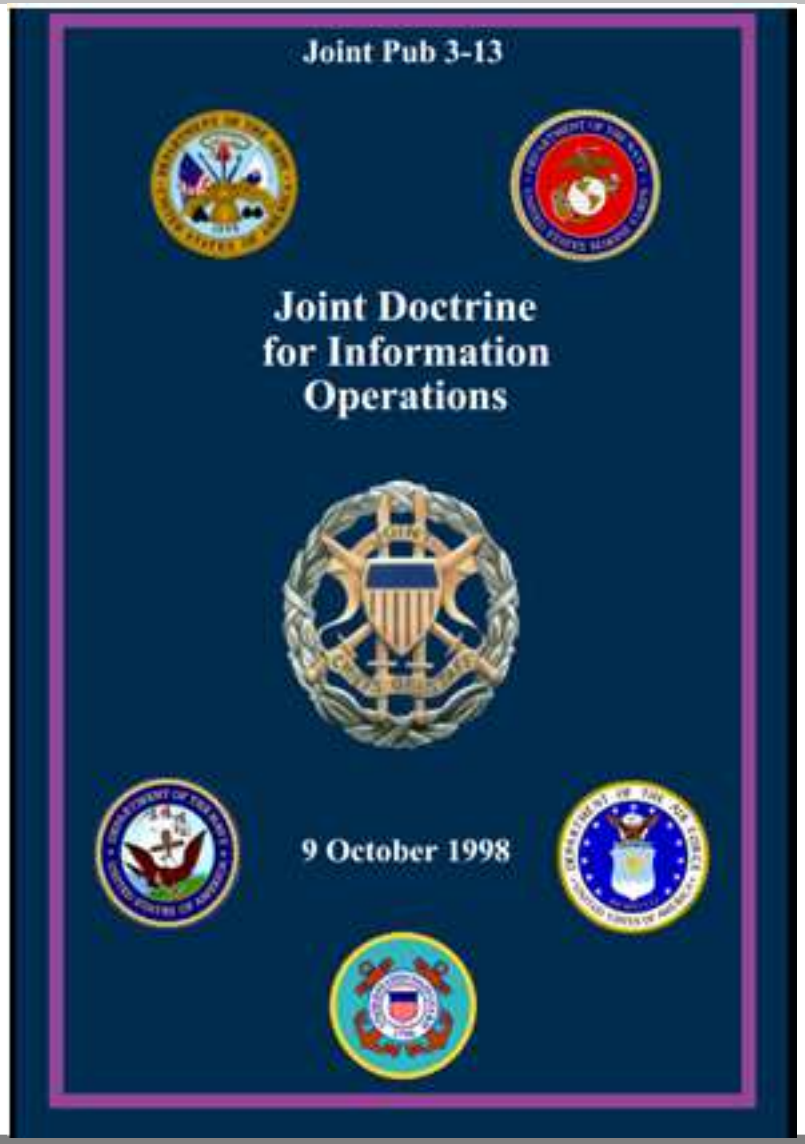
Going after Cybercriminals:

unicri
advancing security, serving justice, building peace

- **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** (those 4 malware factories out there? 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??)

The Way-Future machine

→ **The official one – 1998!**



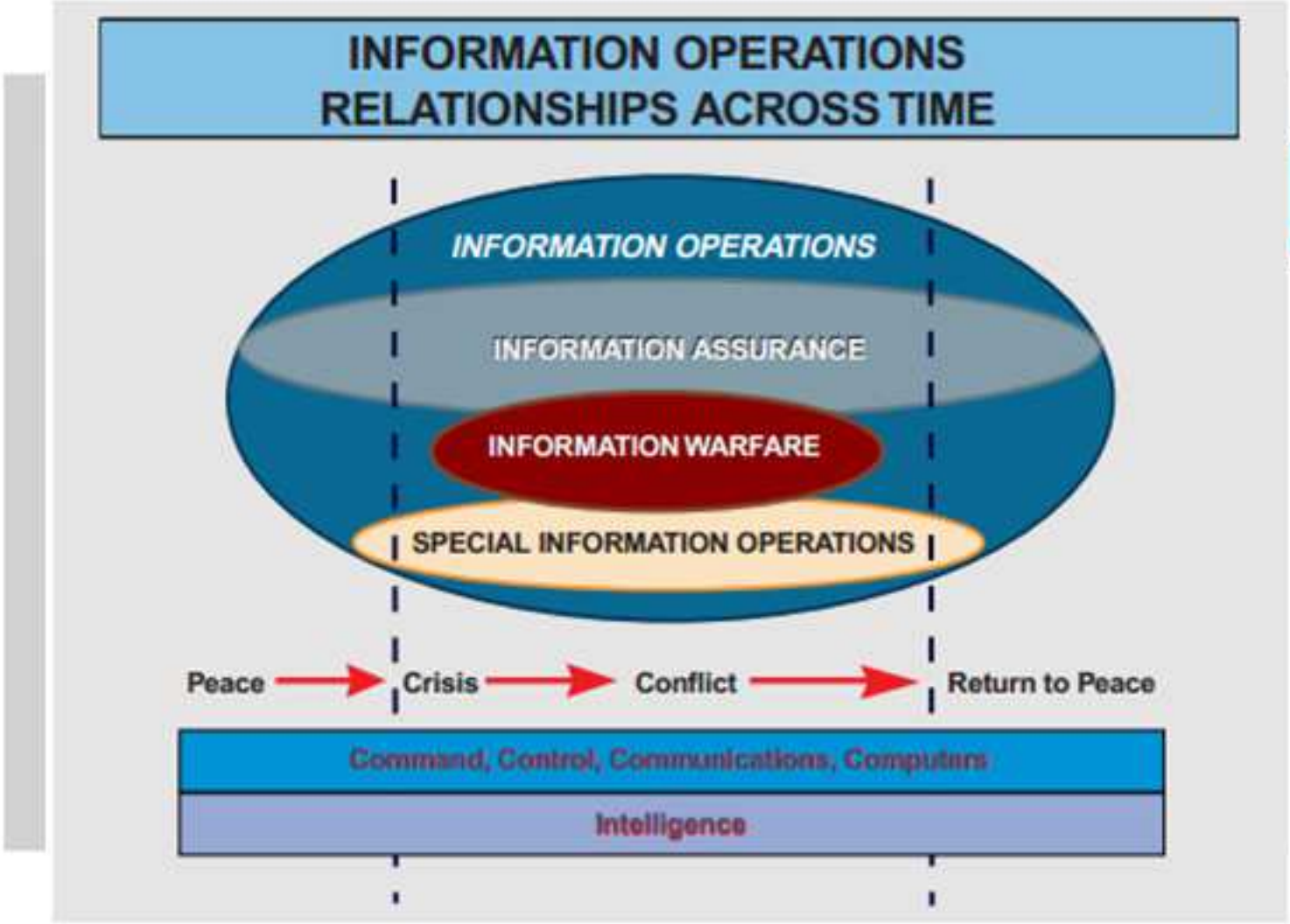
Joint Pub 3-13, "Joint Doctrine for Information Operations," represents a significant milestone in defining how joint forces use information operations (IO) to support our national military strategy. Our ability to conduct peacetime theater engagement, to forestall or peevent crisis and conflict, and to fight and win is critically dependent on effective IO at all levels of war and across the range of military operations.

Joint Pub 3-13 provides the doctrinal foundation for the conduct of IO in joint operations. It discusses integration and synchronization of offensive and defensive IO in the planning and execution of combatant commanders' plans and operations to support the strategic, operational, and tactical levels of war. The guidance contained herein provides joint force commanders and their component commanders with the knowledge needed to plan, train for, and conduct IO.

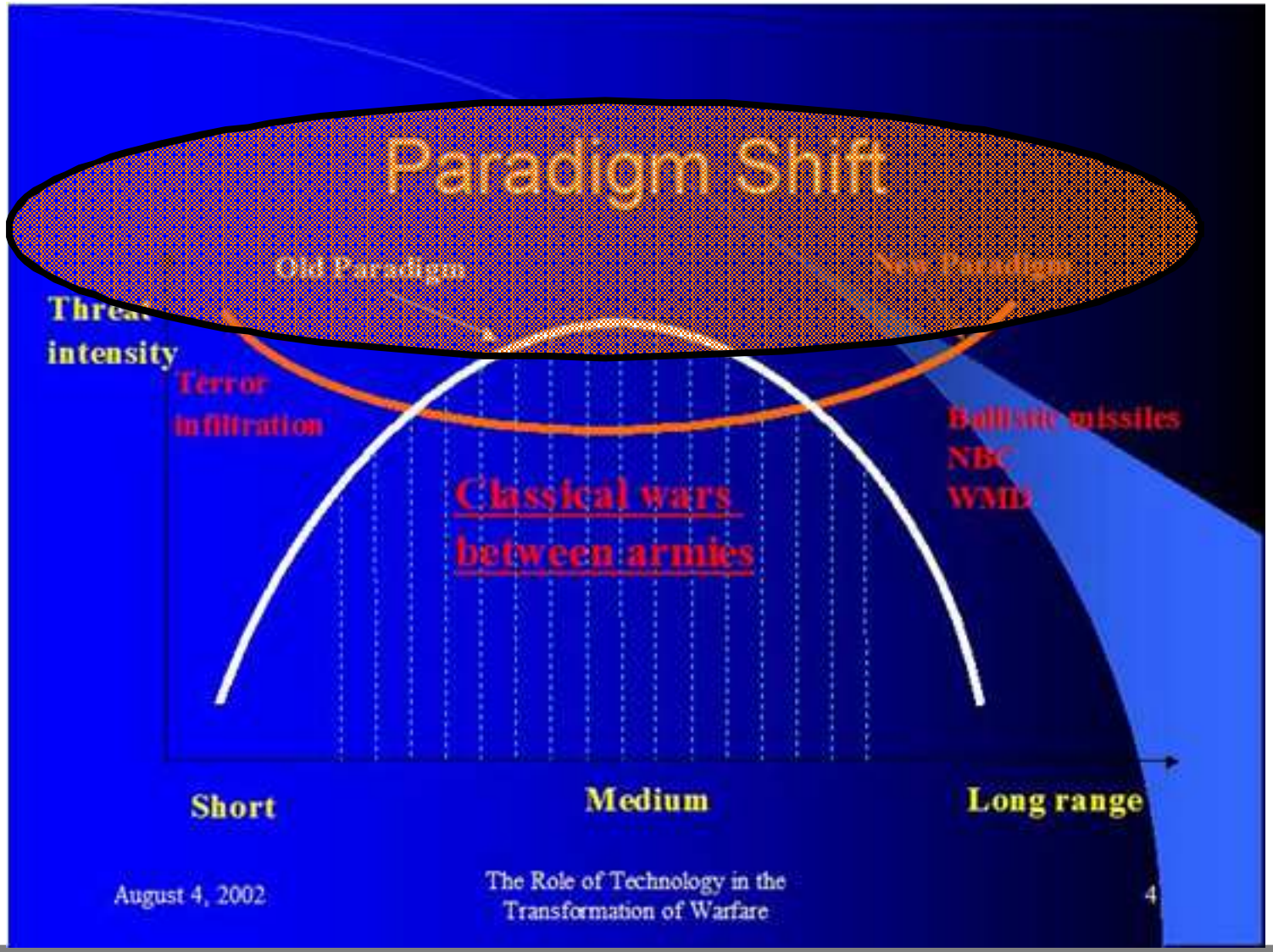
Commanders must understand the content of this publication and bring it to bear during joint and multinational operations. Please ensure the widest distribution of this and other joint publications, and promote their use at every opportunity.

HENRY H. SHELTON
Chairman
of the Joint Chiefs of Staff

→ **The official one – 1998!**



→ **Then, in 2002…**


Paradigm Shift
Old Paradigm
New Paradigm
Threat intensity
Terror infiltration
Classical wars between armies
Ballistic missiles
NBC
WMD
Short
Medium
Long range
August 4, 2002
The Role of Technology in the Transformation of Warfare
4

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.

→ …revised in 2011…

	China	India	Iran	N. Korea	Pakistan	Russia
Official CW doctrine	X*	X*				X*
CW training	X*	X*	X*	X	X*	
CW exercises/simulation	X*	X*				
Collaboration with IT industry/or technical university	X	X*	X*		X*	X*
IT road map		X*	X			
Information warfare units	X*	X*		X*		
Record of hacking other nation	X*		nb		nb	X*

→ **Then, things started to change… (2004-2012)**

Feds Seek a Few Good Hackers

War on terrorism distracts cybercops from routine hacking, and even encourages alliances.

By Andrew Brandt, PCWorld Aug 4, 2004 4:00 am

Attention, hackers: Uncle Sam wants you.

And hackers are answering the call, or at least listening. A well-attended session at the recent Defcon 12 hackers' conference was "Meet the Feds," a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would-be cybercops.

"We're looking for good, talented people. We need a lot of help," said Jim Christy, director of the Defense Department's Cyber Crime Center.

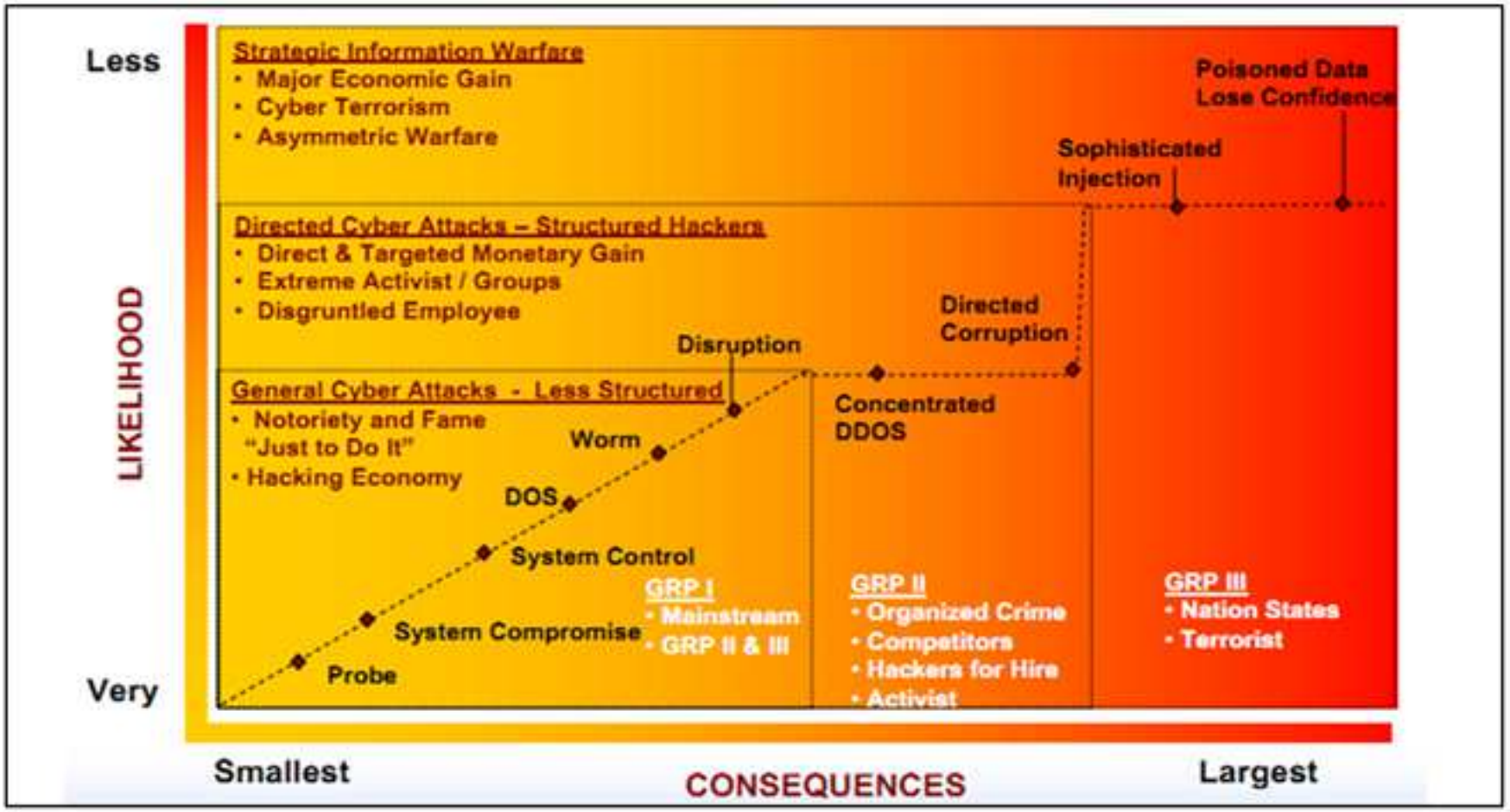
"The Department of Defense understands how important computers are to defending the United States, and is always on the lookout for good people," said Alvin Wallace, a supervisory special agent with the Air Force's Office of Special Investigations.

Patriotic Hackers Sought

→ **Then, things started to change… (2004-2012)**

→ ..and changed a «little bit» more…

Threats are increasing in **severity** and **probability of occurrence**. The advent of concrete Cybersabotage and Cyberware scenarios is strongly rising the risk of **serious** accidents.



→ ..and changed a «little bit» more… (2009-2012)

The UK government has today published its 2011 Cyber Security Strategy.

With an increased focus on cybercrime, and renewed focus on cyberspace as an engine of economic and social prosperity, the strategy continues to hone Whitehall's understanding of this vibrant, complex and increasingly global domain.

Many of the strategy objectives - in particular those related to securing critical infrastructure - will require close engagement with the private sector.

These public-private partnerships are essential, and, as noted in a recent Chatham House report on critical national infrastructure, they require awareness, engagement and trust among senior decision makers on all sides.

This is not an easy process and requires a keen understanding of the incentives that guide actions in the public and private sectors.

Links to business

The government will also have to balance the tension between building a more secure environment - which requires standards and regulation - and encouraging businesses to set up shop in the UK.

However there are signs that Whitehall is aware of these complexities and the need to experiment with potential solutions.

One new initiative is a three-month pilot scheme among five business sectors: defence, finance, telecommunications, pharmaceuticals, and energy.

The UK government plans "unprecedented co-operation" with businesses to improve cybersecunty

Related Stories

- Cyber plan 'to protect UK online'
- FBI downplays water supply 'hack'
- Russia and China 'top cyberspies'

→ ..and changed a «little bit» more… (2009-2012)

The New York Times

U.S.

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

POLITICS EDUCATION

Politics E-Mail

Keep up with the latest news from Washington with the daily Politics e-mail newsletter.

Sign Up

See Sample | Privacy Policy

CYBERWAR

Contractors Vie for Plum Work, Hacking for U.S.

By CHRISTOPHER DREW and JOHN MARKOFF
Published: May 30, 2009

MELBOURNE, Fla. — The government's urgent push into cyberwarfare has set off a rush among the biggest military companies for billions of dollars in new defense contracts.

SIGN IN TO RECOMMEND

COMMENTS (44)

SIGN IN TO E-MAIL

→ **And then, changed a lot more! (2009-2012)**

FT.com FINANCIAL TIMES

Europe

FT Home > World > Europe

- Front page
- World
  - Global Economy
  - US & Canada
  - Europe
    - Brussels
    - European comment
  - UK
  - Asia-Pacific
  - Middle East
  - Africa
  - Americas
  - Columnists
  - Week Ahead
  - Week in review
- Companies
- Markets

Kremlin-backed group behind Estonia cyber blitz

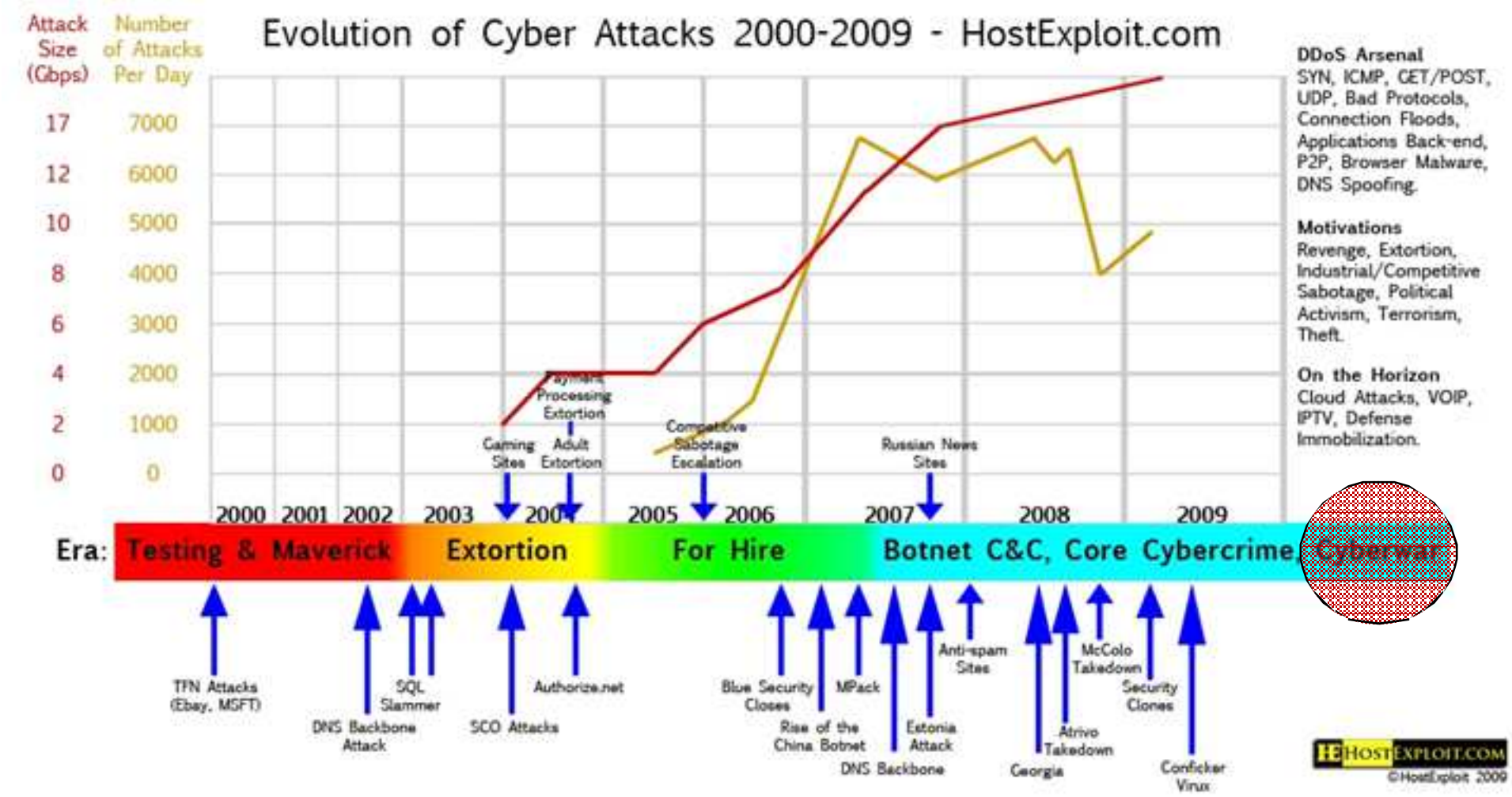
By Charles Clover in Moscow
Published: March 11 2009 02:00 | Last updated: March 11 2009 02:00

Members of a Kremlin-backed youth movement have claimed responsibility for May 2007 cyber attacks that crippled Estonia's internet in the midst of a diplomatic argument with Russia.

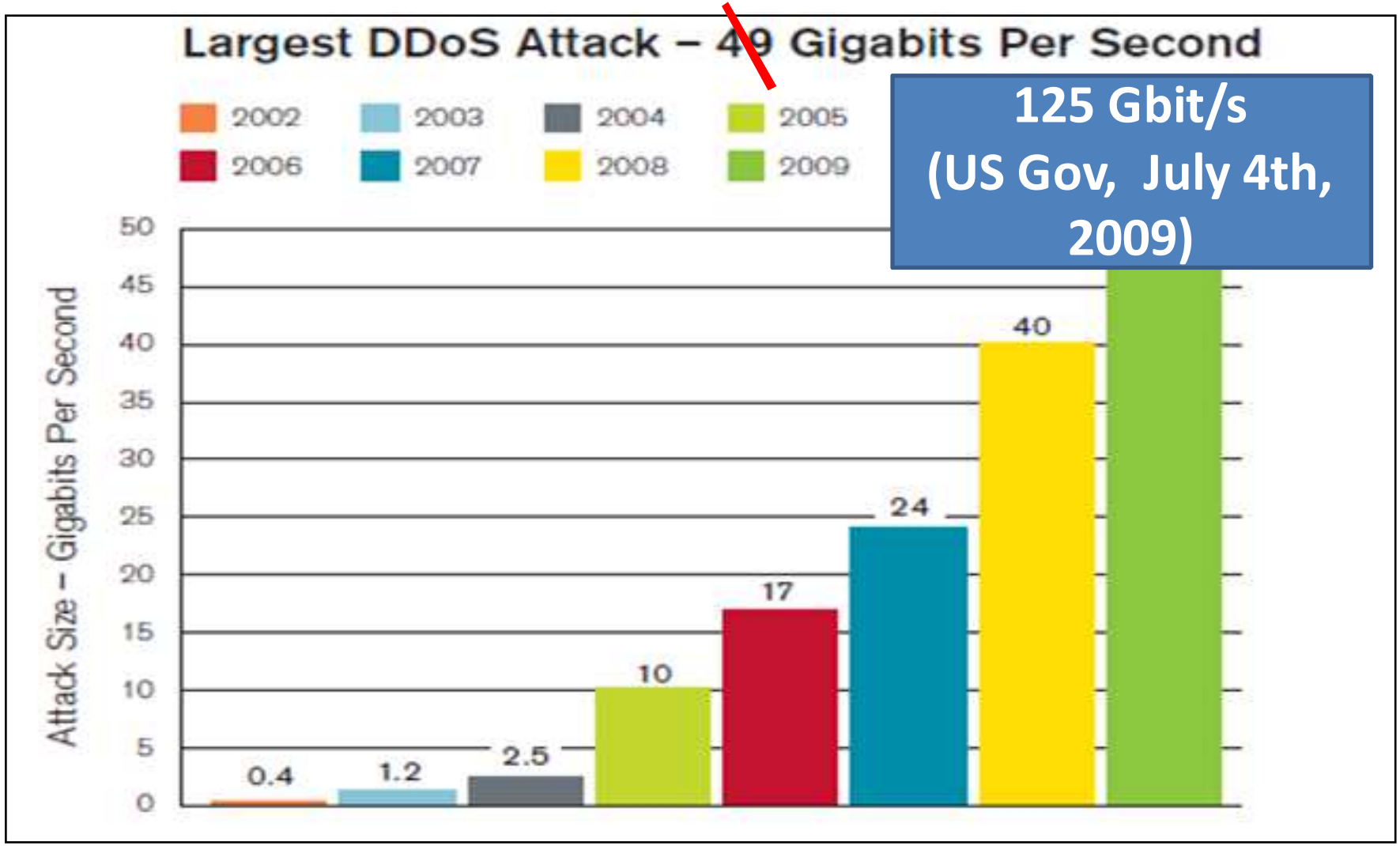
It is believed to have been the first attack of its kind, directed against virtually the entire informational infra-structure of a Nato country.

Estonian officials said the attacks originated in Russia. They began after April 27, when Estonia removed a second world war Soviet memorial from its capital, Tallinn, provoking a storm of protest from Moscow. They continued to mid May.

→ (again) – What's happened?



→ (againx2) – What's happened?




mobile technology
social media
corporates
CRIME
ESPIONAGE
cyber warfare
WikiLeaks
spies
ISPs
anonymization
data retention
The Hacker
ordinary folk
social engineering
software piracy
net neutrality
deception
law enforcement
press freedom
POWER
civil liberties
state control

→ **Now it's 2012.**

WIRED SUBSCRIBE SECTIONS BLOGS REVIEWS VIDEO HOW-TOS

DANGER ROOM

WHAT'S NEXT IN NATIONAL SECURITY

PREVIOUS POST NEXT POST

Obama's New Defense Plan: Drones, Spec Ops and Cyber War

793 38 68

Tweet +1 Share

By Spencer Ackerman January 5, 2012 | 12:57 pm | Categories: Tactics, Strategy and Logistics

Follow @attackerman

Like Send 197 people like this.

The President announced his vision for the future of the U.S. military today. Kiss big counterinsurgencies goodbye. Get ready for more shadow wars, drone attacks and online combat, with the military's eyes on the Pacific, rather than Afghanistan.

In a rare visit to the Pentagon, President Obama declared that the U.S. will be "strengthening our presence in the Asia-Pacific," while "turning the page on a decade of war." In practice, that means cutting the Army and Marine Corps and unspecified "outdated Cold War systems," part of a broad effort to cut what the Pentagon

→ **Now it's 2012.**


threatpost

The Kaspersky Lab Security News Service

Wednesday, May 23rd, 2012

Search

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Governm

Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vuln

Home › Hacks ›

May 18, 2012, 3:34PM

Defense Contractor Northrop Grumman Hiring For Offensive Cyber Ops

by Paul Roberts

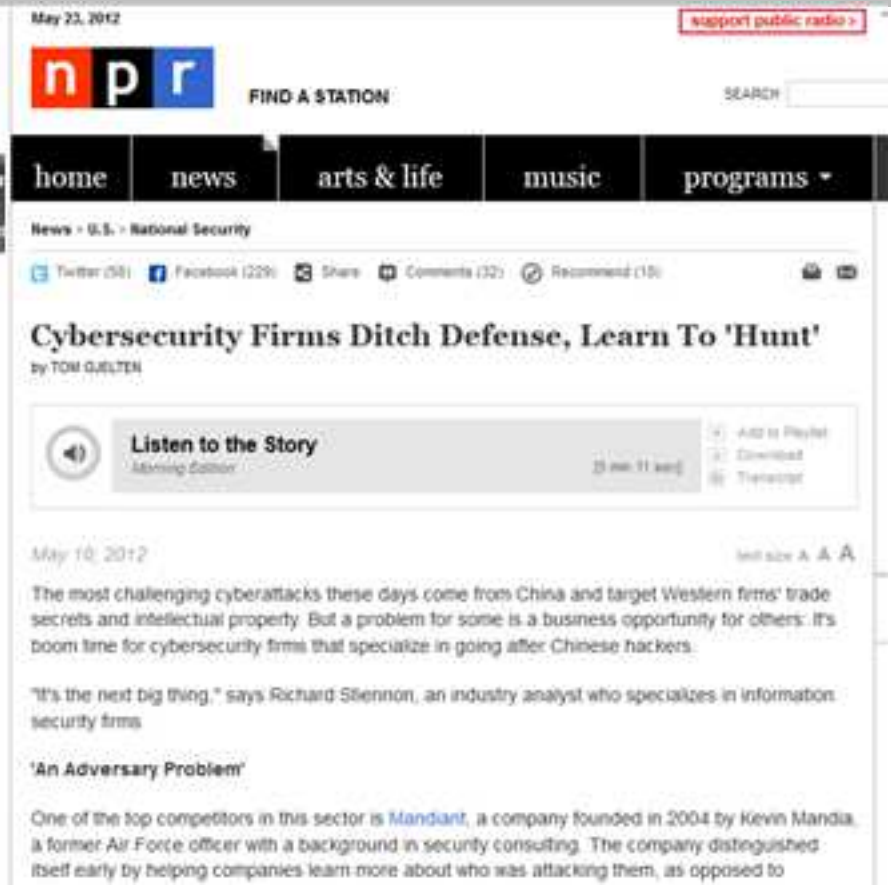
Follow @paulfroberts

10 Comments

Defense giant Northrop Grumman is hiring software engineers to help it carry out "offensive cyberspace operations," according to a recent job posting.

The job posting, for a "Cyber Software Engineer 2" appeared on the Website Clearancejobs.com and described a position on a Northrop R&D project to "plan, execute and assess an Offensive Cyberspace Operation (OCO) mission" that would include familiarity with tools like Metasploit and Google Earth and "integration of capabilities such as command linkages, data flows, situation awareness (SA) and command and control (C2) tools."

http://threatpost.com/en_us/blogs/defense-contractor-northrop-grumman-hiring-offensive-cyber-ops-051812


May 23, 2012

support public radio

npr

FIND A STATION

SEARCH

home | news | arts & life | music | programs

News › U.S. › National Security

Twitter (58) Facebook (229) Share Comments (32) Recommend (15)

Cybersecurity Firms Ditch Defense, Learn To 'Hunt'

by TOM GJELTEN

Listen to the Story

Morning Edition

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'

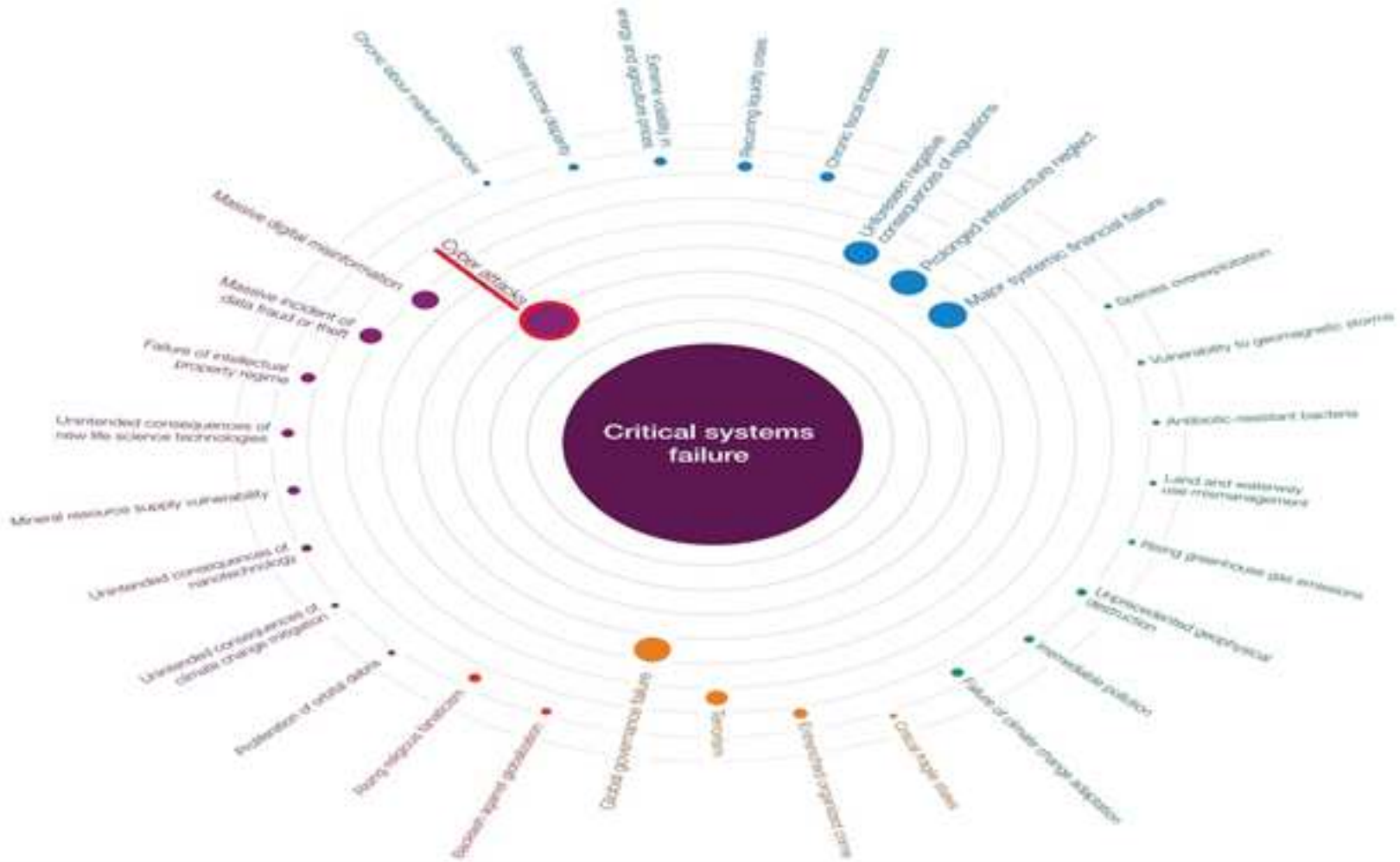
One of the top competitors in this sector is Mandiant, a company founded in 2004 by Kevin Mandia, a former Air Force officer with a background in security consulting. The company distinguished itself early by helping companies learn more about who was attacking them, as opposed to

http://www.npr.org/2012/05/10/152374358/cybersecurity-firms-ditch-defense-learn-to-hunt

→ WEF Report 2012

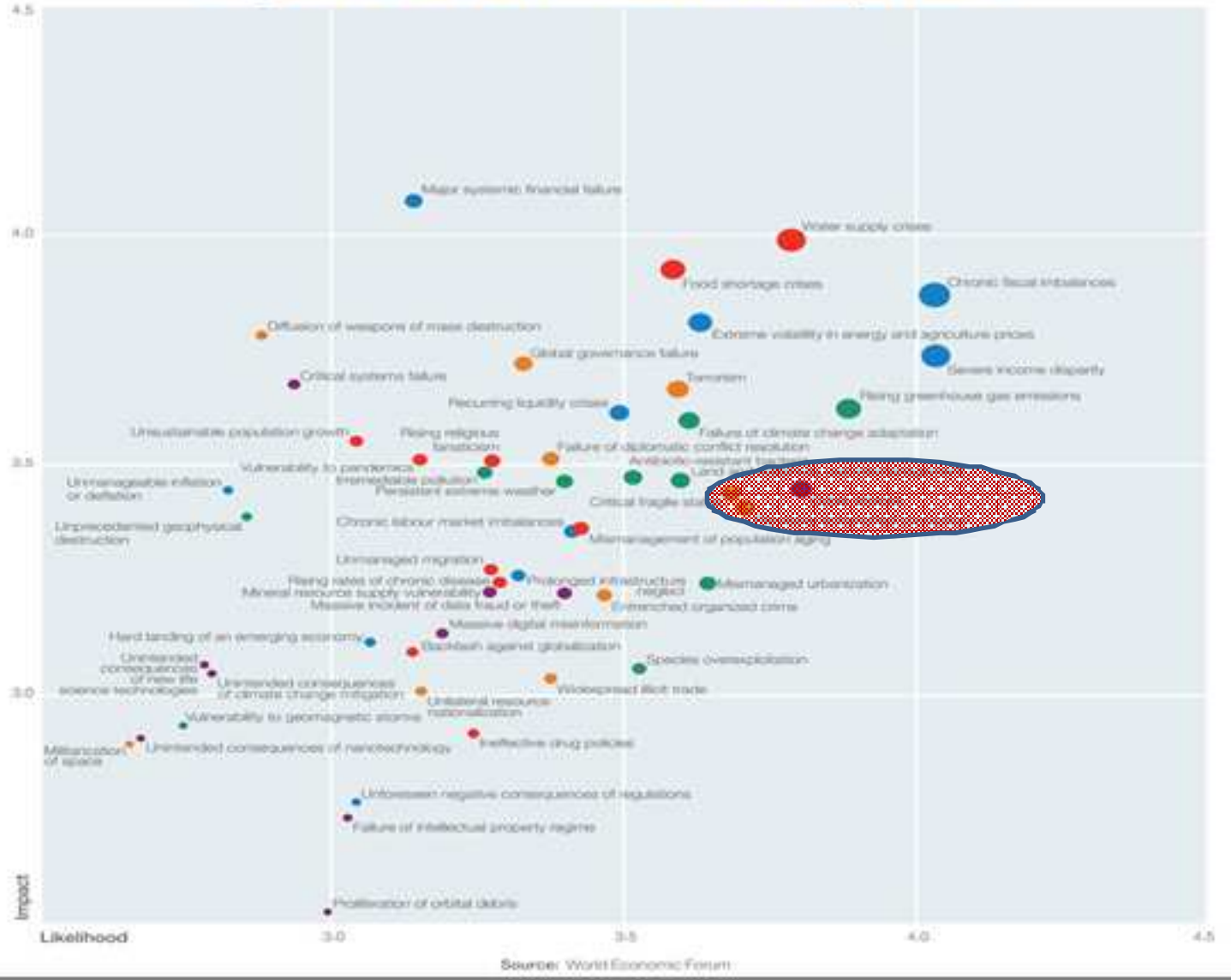
WORLD ECONOMIC

Figure 39: Critical Systems Failure is the Centre of Gravity in the Technological Category



→ **WEF Report 2012**

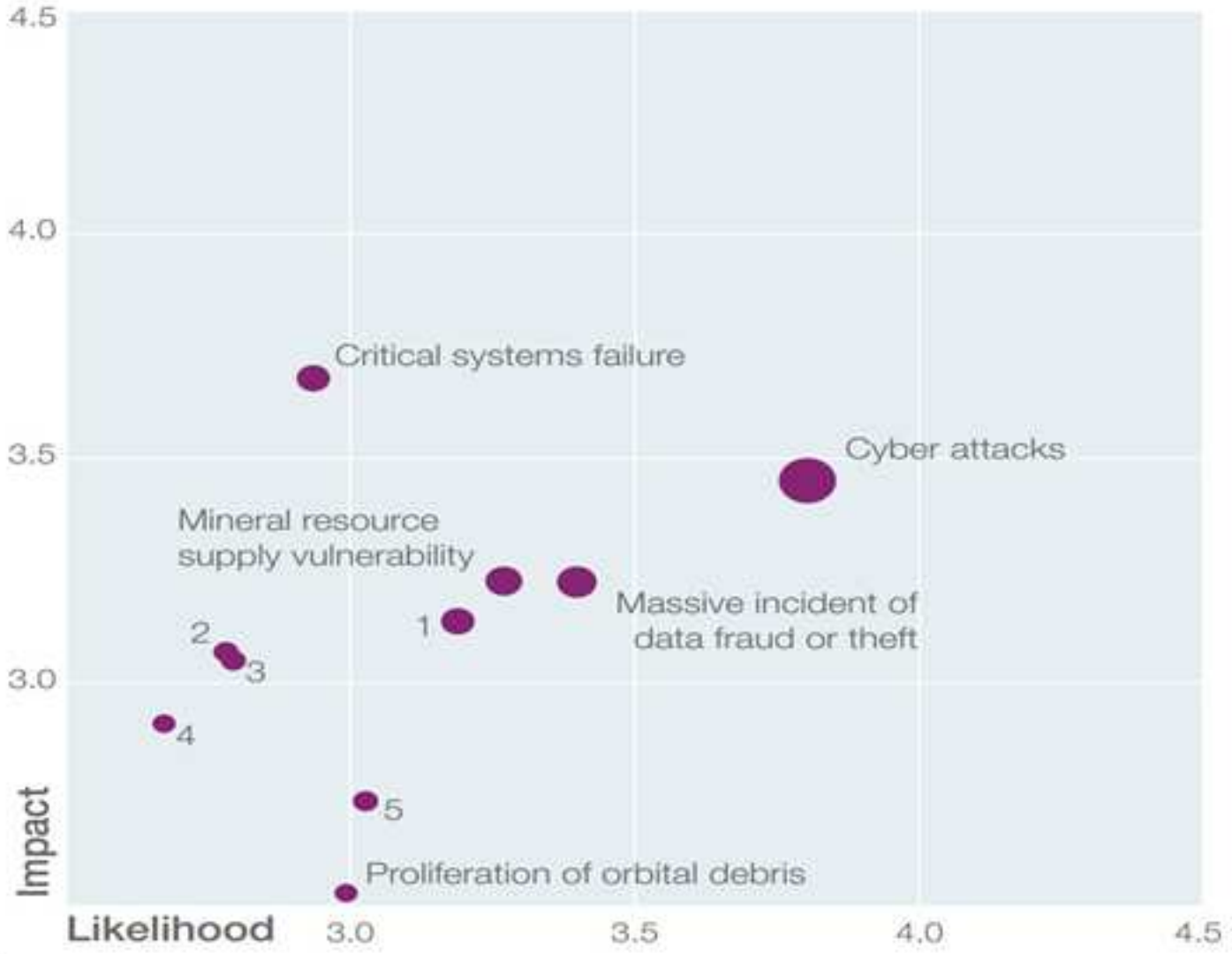
Figure 2: Global Risks Landscape 2012



Source: World Economic Forum

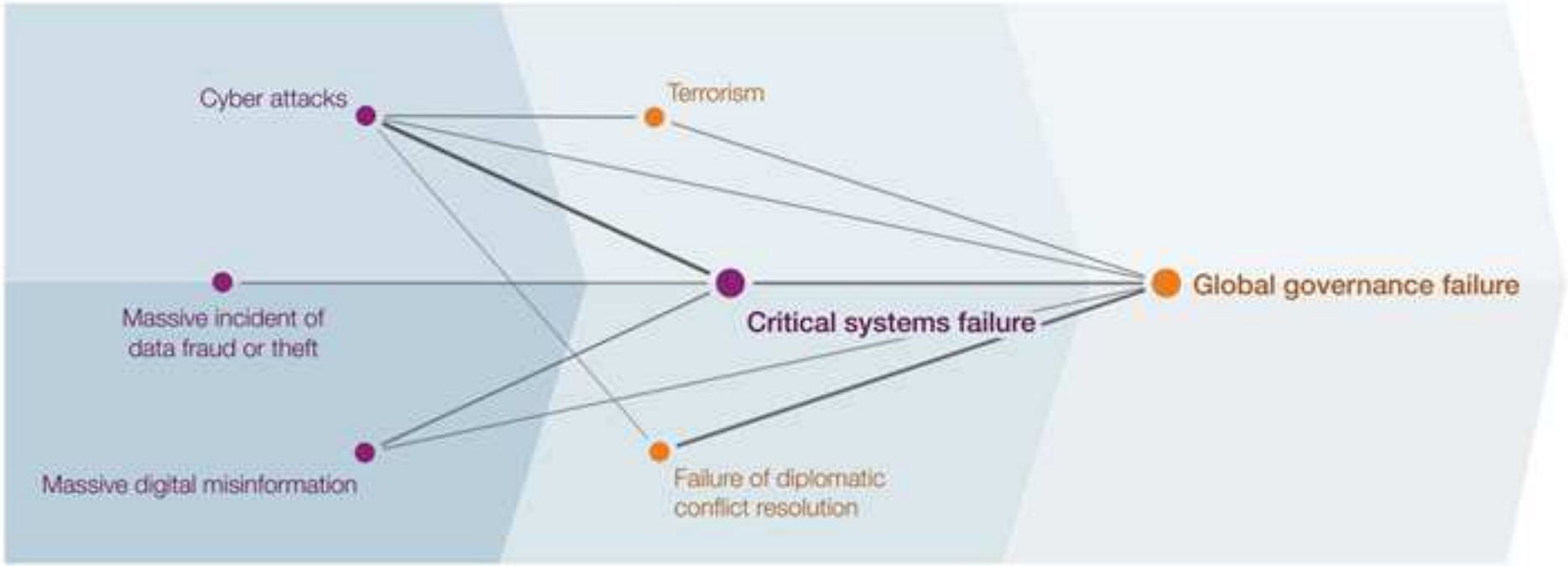
→ **WEF Report 2012**

Figure 38: Technological Risks



→ WEF Report 2012

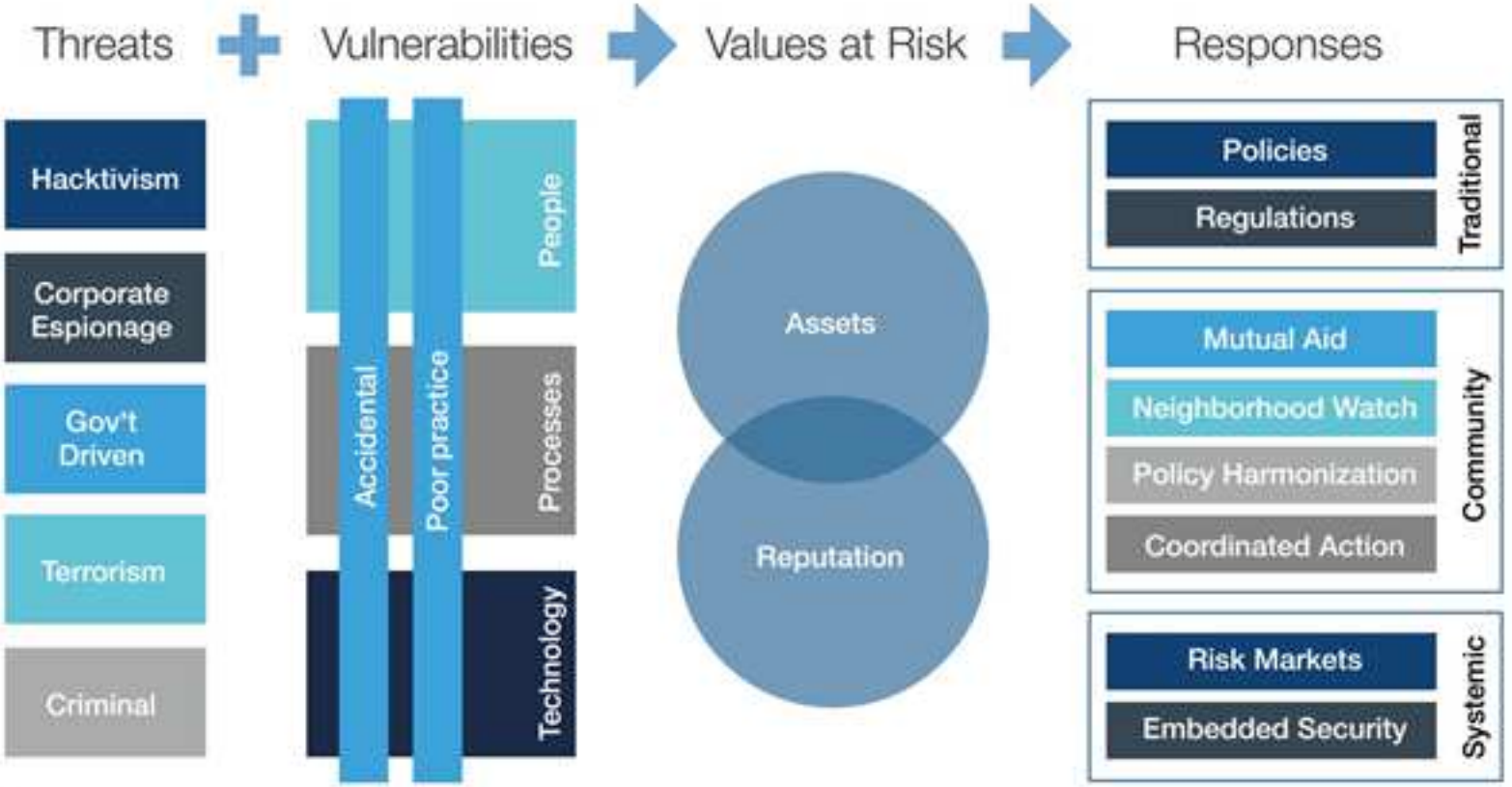
Figure 17: The Dark Side of Connectivity Constellation



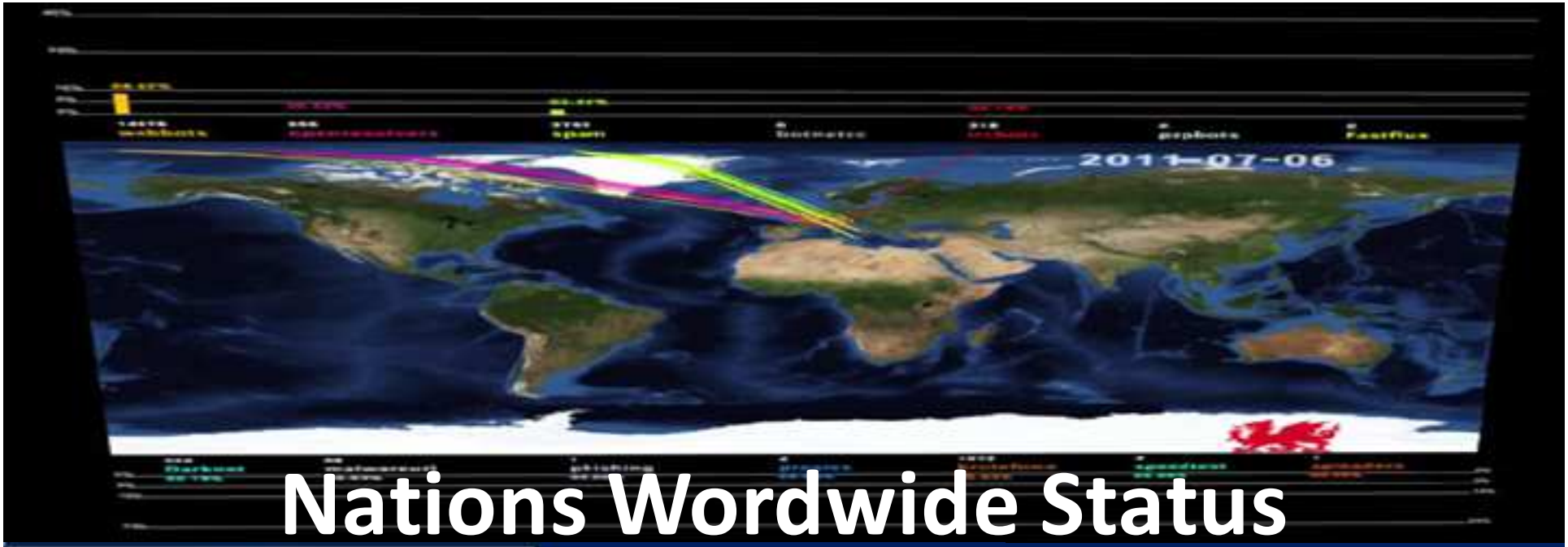
Source: World Economic Forum

→ **WEF Report 2012**

Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum



Nations Wordwide Status

→ From the «past» IT and InfoSec we all used to know…

* Just as you **started getting used of these words** over the years…

* **"Paranoia" (that's into your DNA, hopefully!)**
* **"Information Security" (198x)**
* **"Firewall", "DMZ" (1994/5)**
* **"Pentesting" (1996/7)**
* **"xIDS" (2001-2003)**
* **"Web Application Security" (2006-2009)**
* **"SCADA&NCIs" (2008-201x)**
* **"PCI-DSS" (2009-201x)**
* **Botnets (2008-2010)**
* **"APTs" (2011-201x)**
* **etc…**

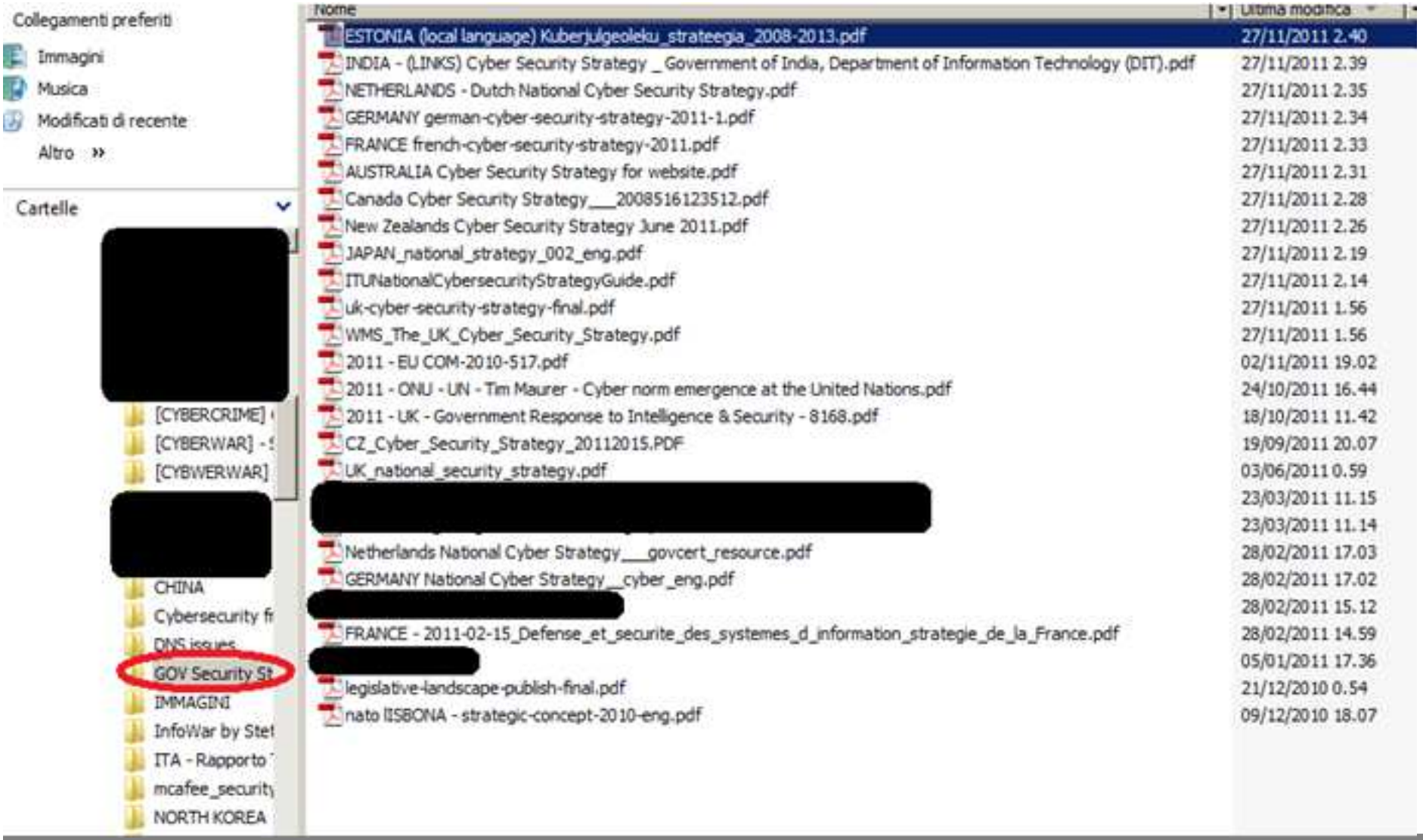
→ …through today…

→ ..into the «future» of our countries and lives

* …in the next (two to five) years, you will hear non-stop talks about:

  * NGC – Next Generation Cybercrime
  * Cyber War
  * Information Warfare
  * NGW – Next Generation Warfare
  * PCA - Private Cyber Armies

→ Government Security Strategies – 2012



→ 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[21]		X	X			
Belarus	X		X			
China[21]	X		X	X	X	[illegible]
North Korea[21]			X		X	[illegible]
France[21,29]	X		X	X	X	
India[21, 31]	X		X	X	X	33
Iran[21,][illegible]			X		X	34,35
Israel[21,]	X		X	X	X	
Pakistan[21,][illegible]			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	

In a nutshell:– 2012 (Survey from Jart Armin & Raoul Chiesa – Cyberdefcon Ltd., UK)

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)

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**.*

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

POLENTA DI FARINA GIALLA

POLENTA TARAGNA

- Botnet & drone armies

- DDoS

- Trojans & Worms

- Malware

- Server hacking

- Encryption

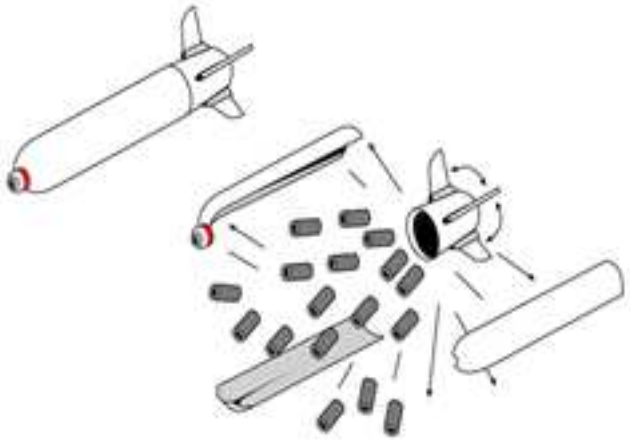
- Extortion & Ransom

- Man in the Middle

Black Energy

Stuxnet

- Cluster Bomb



- Cruise Missile

Black Energy

Multiple targets, loud and noisy

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

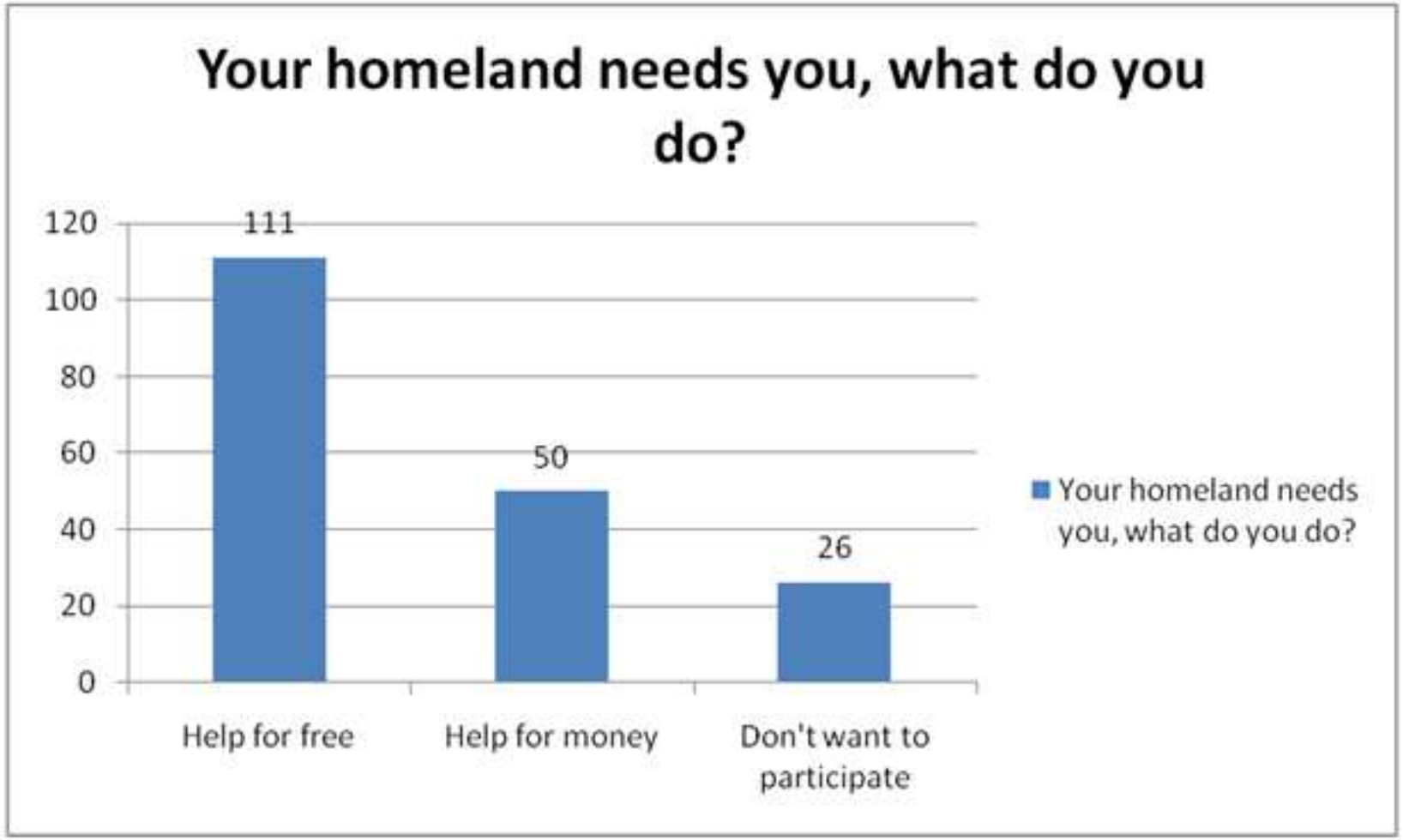
Stuxnet

Laser Guided, precision, and stealth

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


Hackers in the national cyber security
Csaba Krasznay
IT Security Consultant
Hewlett-Packard Hungary Ltd.

→ DIYO as a hobby



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

- **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".

- Recruiting “digital soldier” within 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).

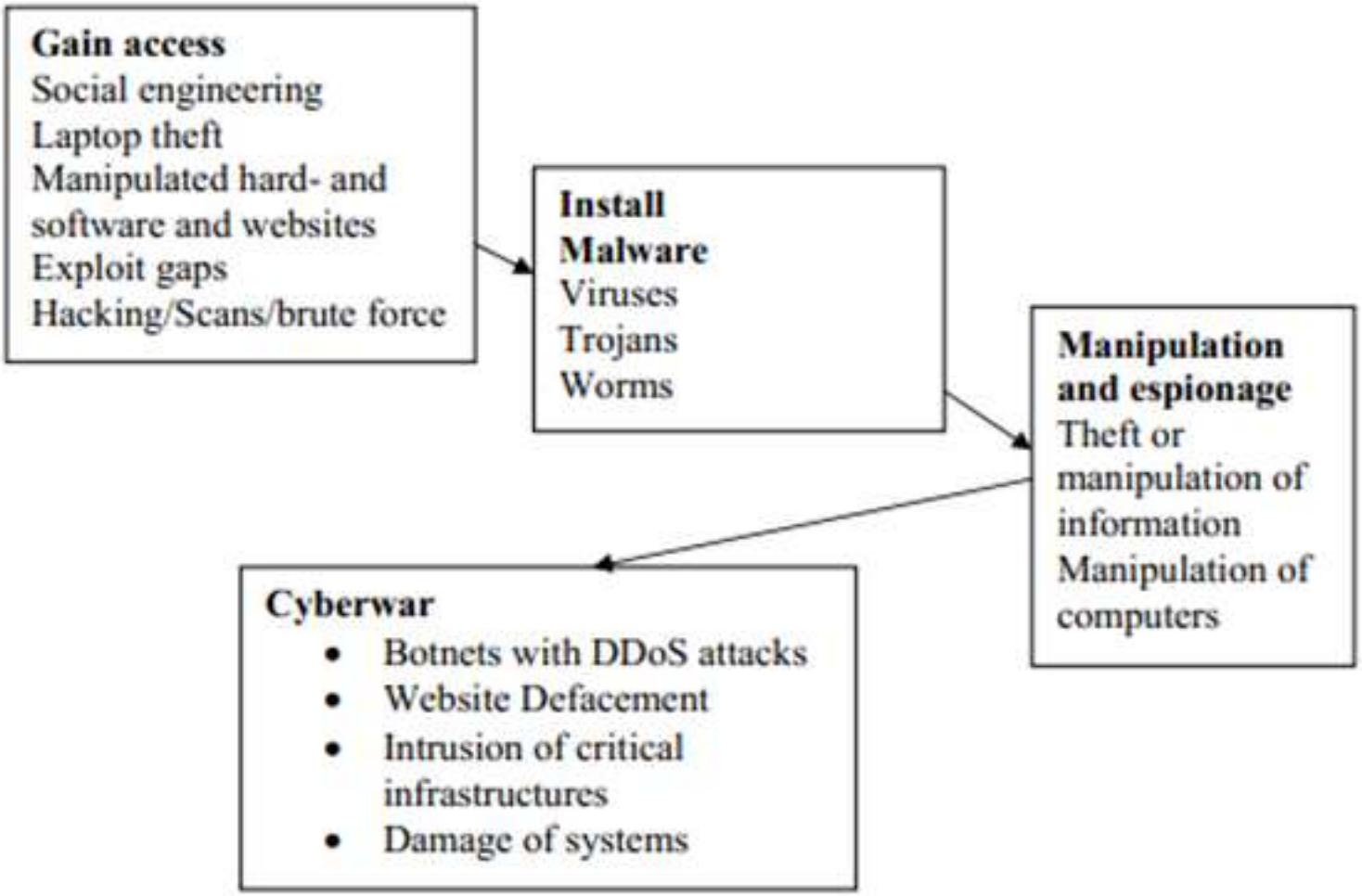
- Concept to quickly and effectively **develop cyber offense capabilities.**
- **Partnership with private security industry** to establish "cyber war capabilities".
- **Enhance** national and foreign **intelligence capabilities** in **cyberspace.**
- **Develop** cyber armaments and digital weapons for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

- 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**.

SLIDE NOT PRESENT IN THE PUBLIC RELEASE OF THIS PRESENTATION
(YOU SHOULD HAVE ATTENDED CONFIDENCE X 2012!)

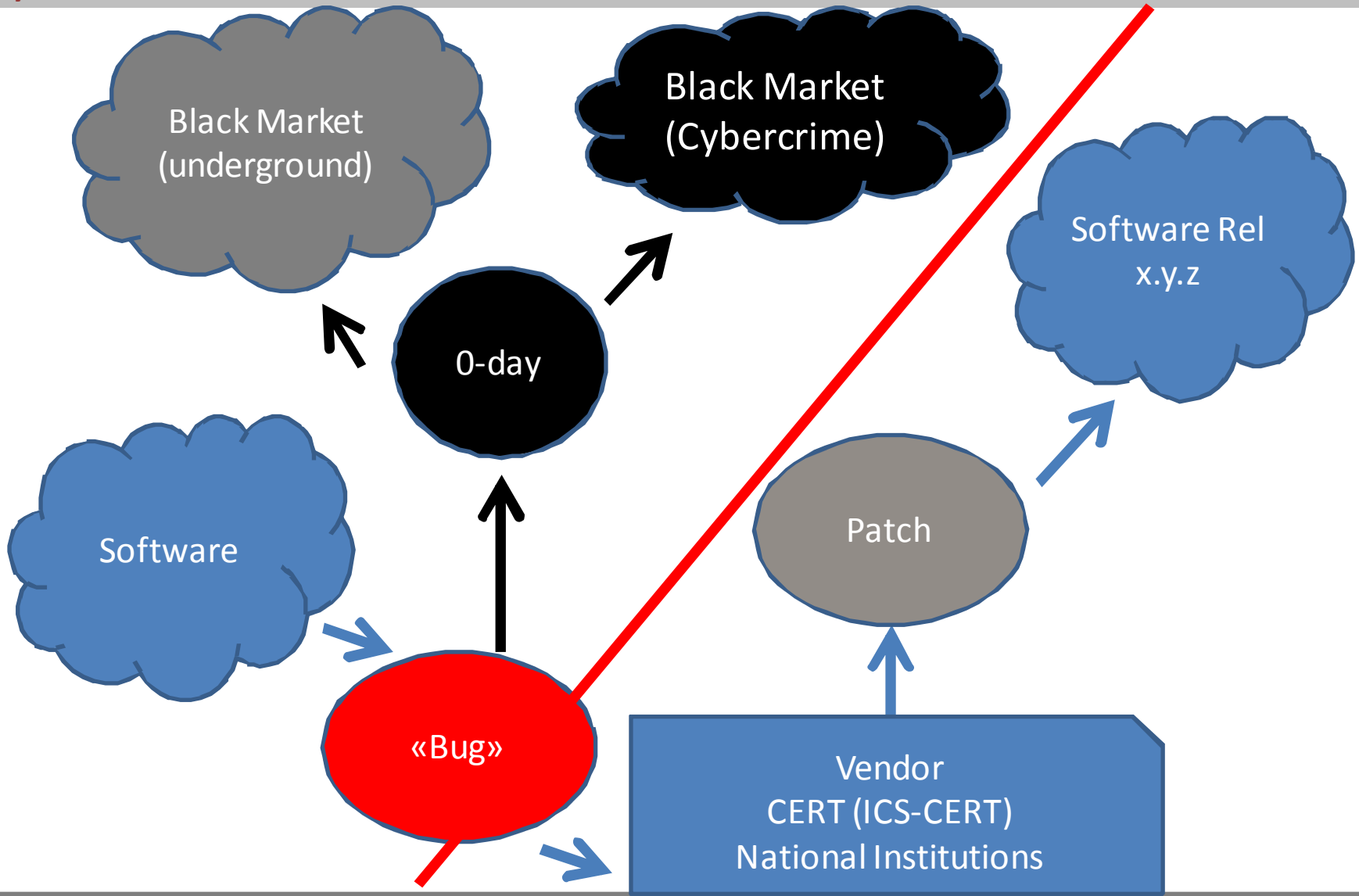
→ Cyber Attack «Methodology», from the Military & DoDs Perspective (March 2012)



Source: Saalbach, Cyberwar Methods & Practice

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

Source: Jim Geovedi, Indonesia


Black Market
(underground)
Black Market
(Cybercrime)
Software Rel
x.y.z
0-day
Software
Patch
«Bug»
Vendor
CERT (ICS-CERT)
National Institutions

→The 0-day market' prices : what official surveys tell us.

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

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

→ 0-day Market prices – hacker's surveys.

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

→ 0-day Market prices – hacker's surveys.

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

→ Budgeting

- **Strategic Governance**
  TBD
- **Operations management unit**
  and
- **Technology R&D unit**

See:

- ✓ http://taosecurity.blogspot.com/2009/06/black-hat-budgeting.html
- ✓ http://taosecurity.blogspot.com/2009/07/white-hat-budgeting.html
- ✓ http://taosecurity.blogspot.com/2010/05/more-on-black-hat-costs.html
- ✓ http://taosecurity.blogspot.com/2009/06/counterintelligence-options-for-digital.html
- ✓ http://english.aljazeera.net/programmes/aljazeeraworld/2011/10/201110191693940 2528.html
- ✓ http://www.govinfosecurity.com/articles.php?art_id=4185

→ **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)***

→ **How such an «organization» would eventually look like?**

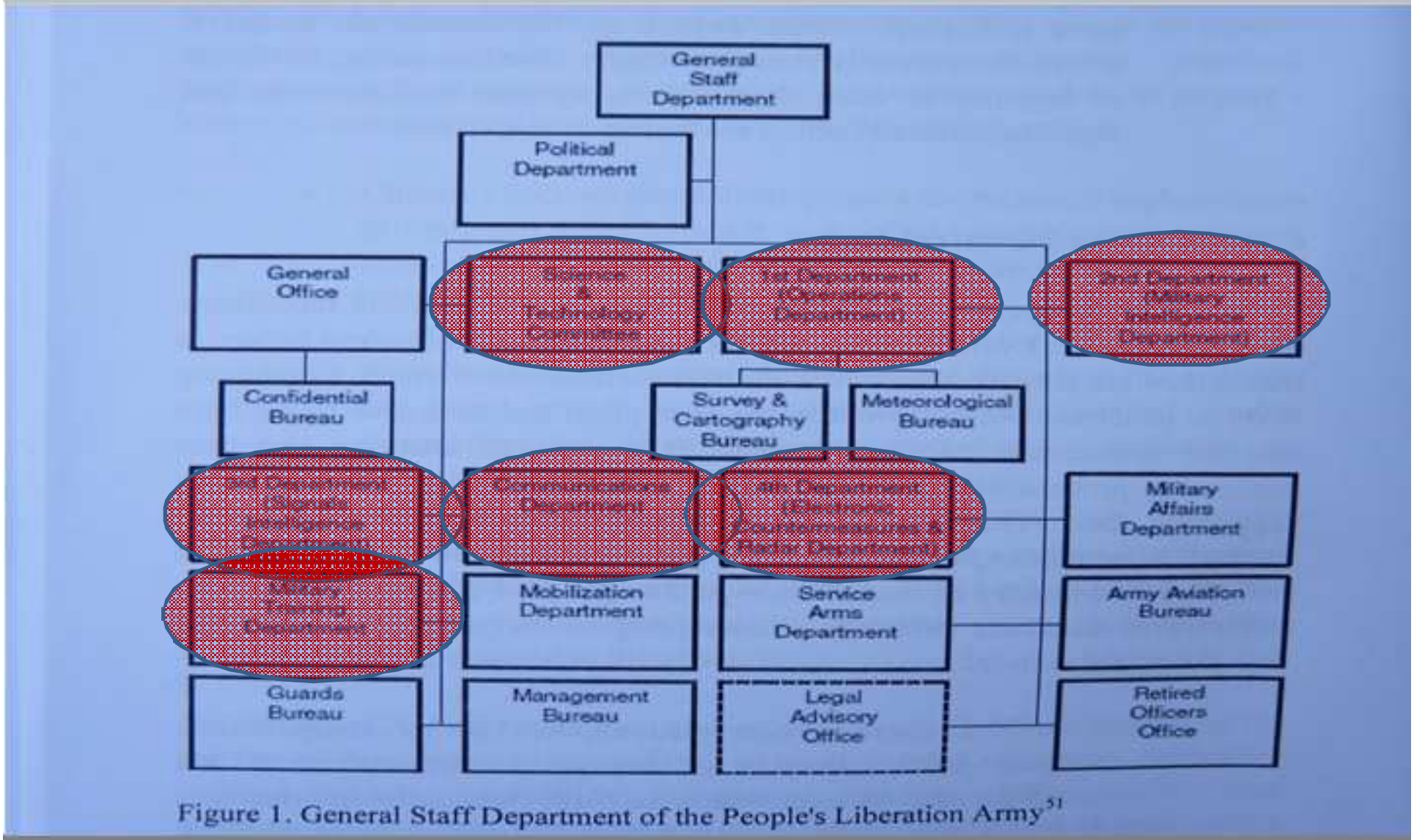
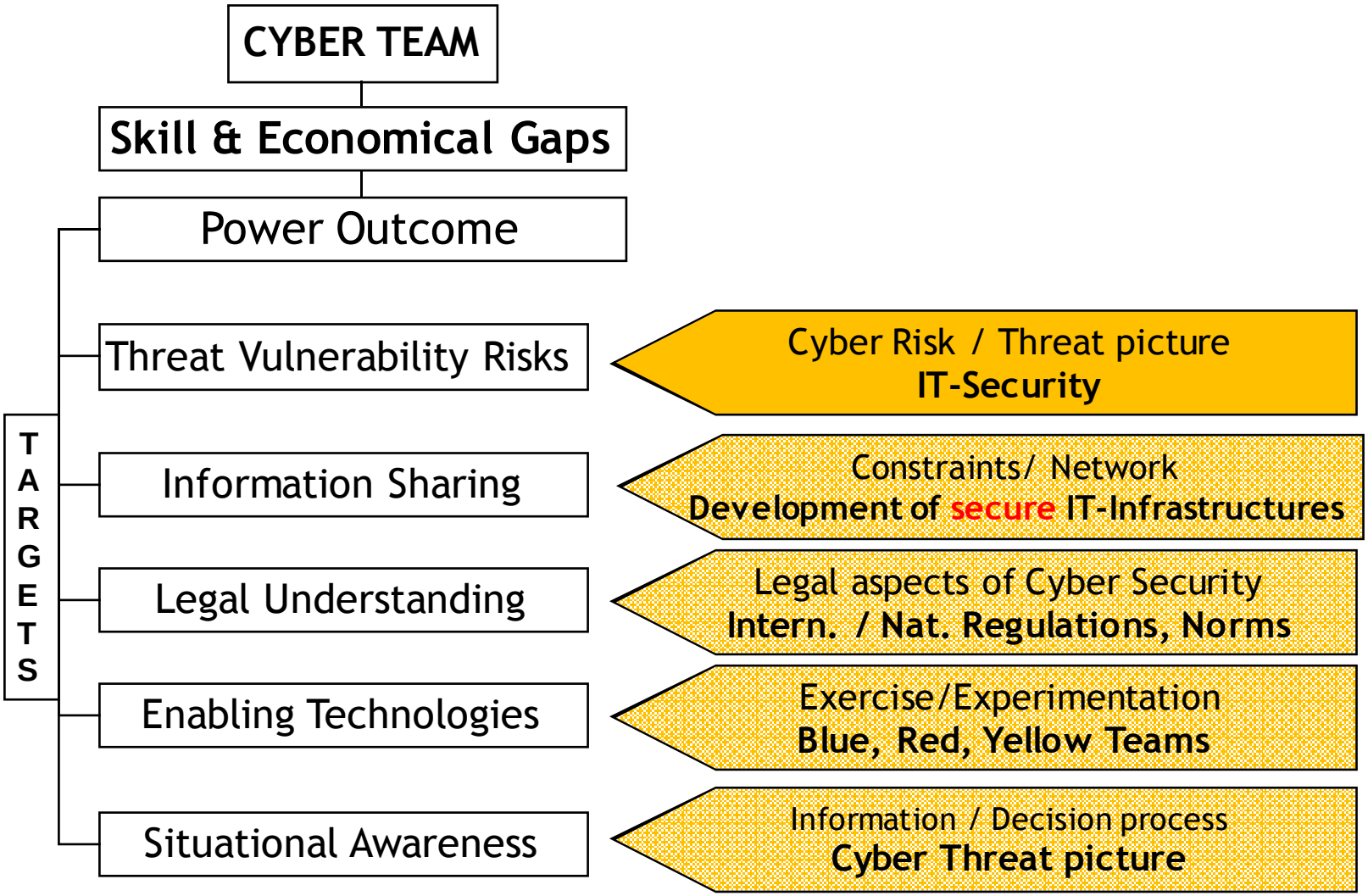


Figure 1. General Staff Department of the People's Liberation Army[51]

→ **Setting up a proper team**

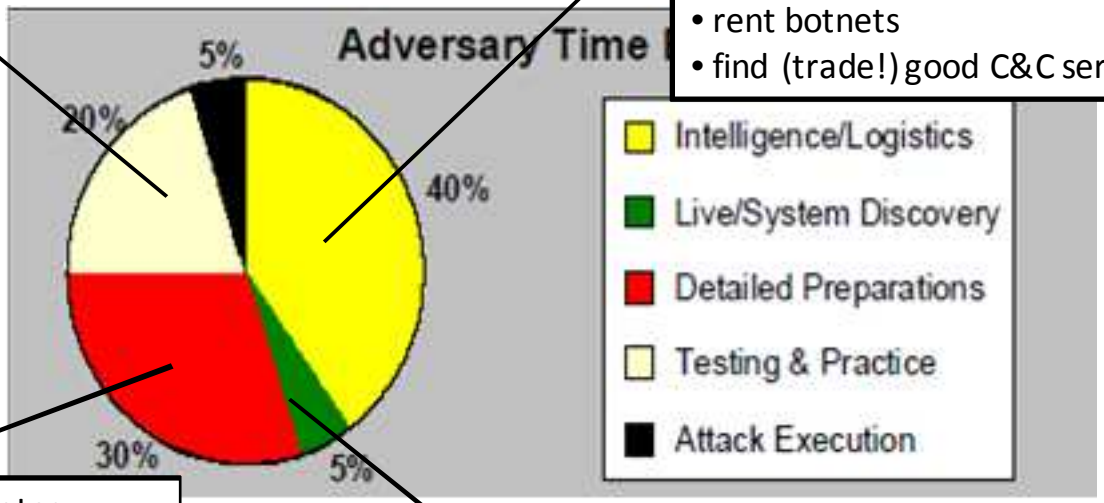


→ Putting all together

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

→ **Plausible different actors, tough… (Non-State CNE [cybercrime] done by State)**

Scenario III: "minor" Cybercrime

Usually either appendixes of existing OC or ind. small investigators

Basic hacking, DDoS, web defacement (besides carding, spam,…)

Can be "cyber-militia", independent criminals → CNE mostly contract

Scenario II: "major" Cybercrime

Major OC, also leverages "minor level" political corruption in LE

"*Kompromat*" (Internet, voice), APT campaigns (R&D /M&A) etc.

Independent targeting + contract / career OC w. LE/IC, academia, etc.

Scenario I: "political" Cybercrime

Internal government Cyber: Mil, IC, LE, i.e., official cyber

All services (primarily IP theft)

"super-empowered" political individuals w. public resources for private

Alexander Klimburg 2012

IC: Intelligence Community OC: Organized Crime LE: Law Enforcement

→ **Putting all together: State CNE done by Non-State actors…**

Scenario I : State *directed* (primarily IC & contracted)

"direct state interest" → targeted, contracted

"convergence" of state / private CNE and CNA objectives

Includes IC and close cooperation of IC / major organized crime (OC)

Scenario II: State *sponsored* (primarily ONSA)

"push" rather than "pull" (active incentives)

"distraction" and "training" benefit of unofficial cyber forces

Both opportunistic and targeted

Scenario III: State *tolerated* (primarily NONS)

"if you want cheap cyberwar, you need cybercrime" (passive incentive)

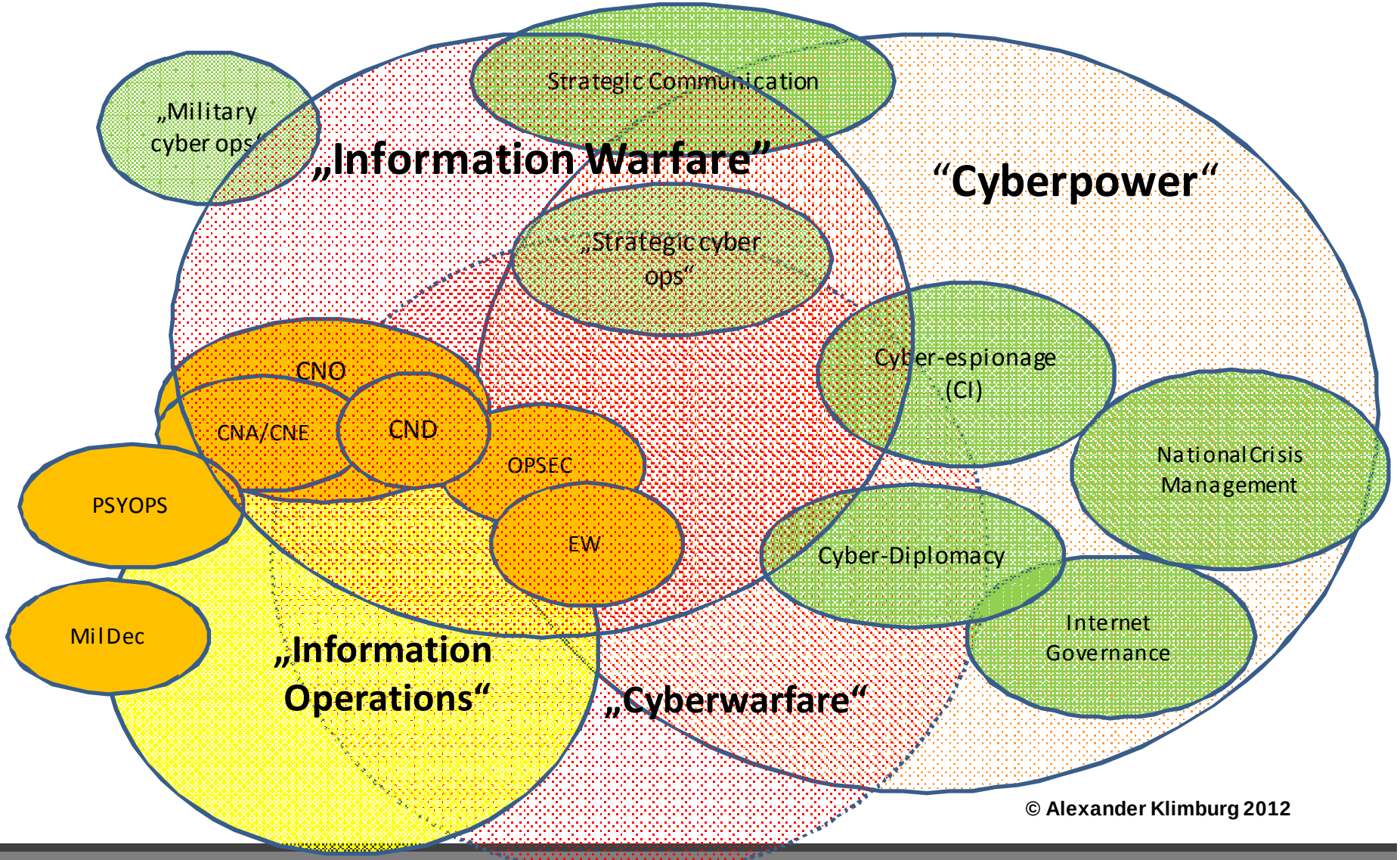
Internal political reasons (divert attention, hostility, lack of LE)

Tolerated at one level often means *sponsored* at another!

Alexander Klimburg 2012

IC: Intelligence Community **ONSA= Organised Non State Actors** **NONS: Non-Organized Non-State**

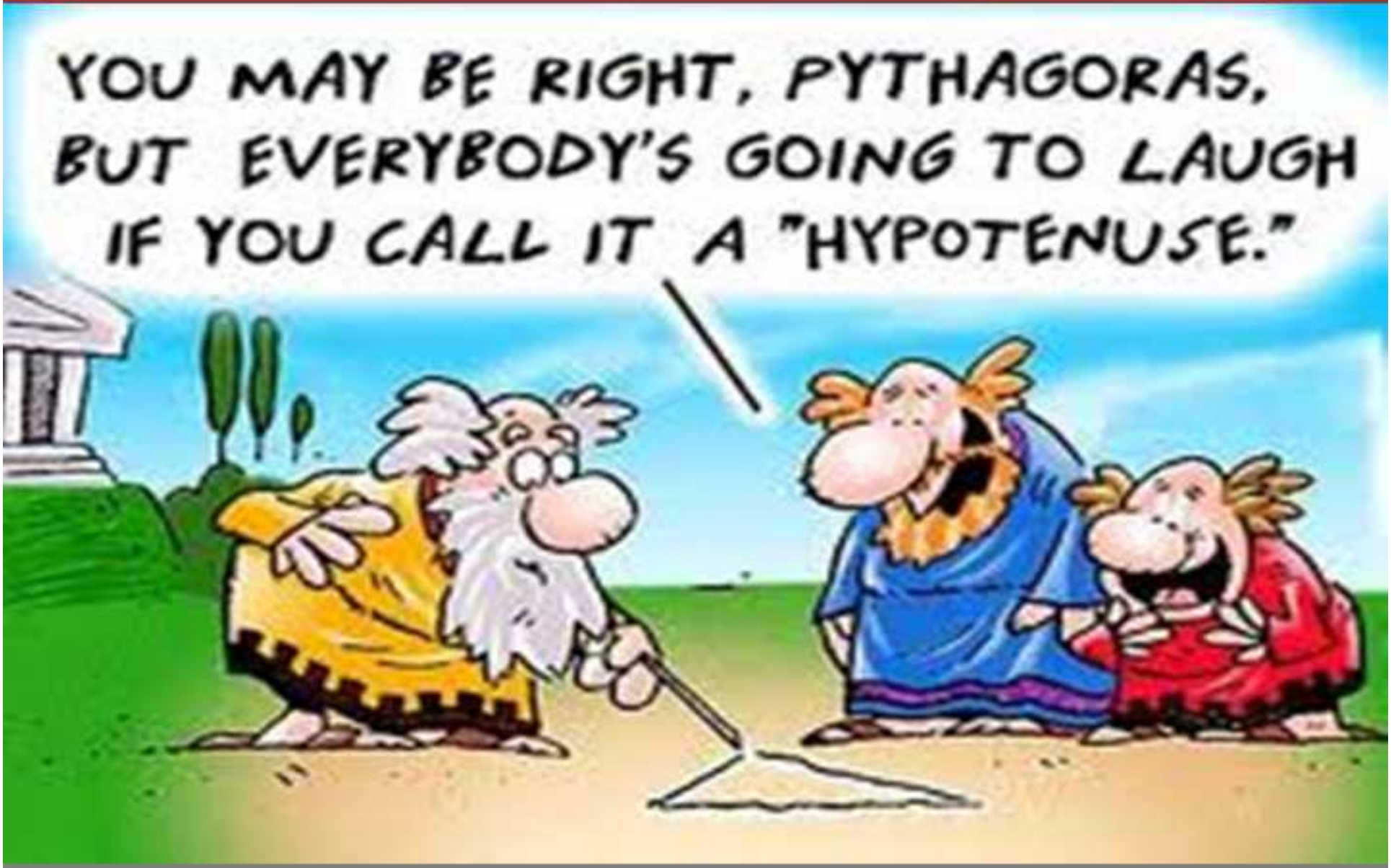
→ **It's outta there. Now.**



→ 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?

Conclusions



→ **Lack of Lingua Franca, components, roles, and rules.**

„**Cybersecurity, Cyber-security, Cyber Security ?**”

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?…

"Cyberpower"

❑"The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."

(Krammer / Starr / Kuehl)

"Cybersecurity" (NO official terms)

❑„Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."

(Netherlands National Cyber Security Strategy)

❑"the protection of data and systems held and transferred in networks that are connected to the Internet".

(**Accenture**)

→ 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

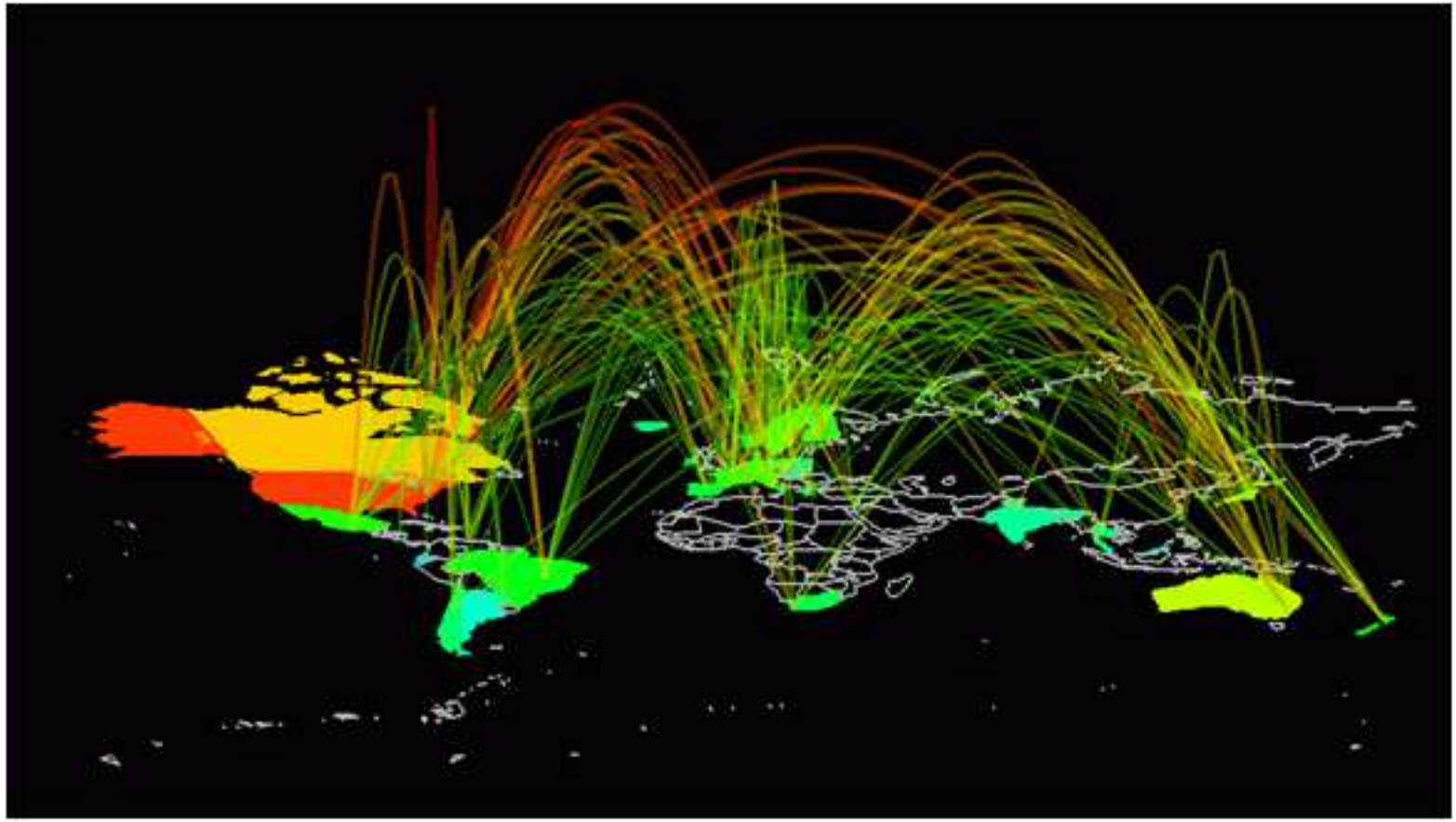
Strategy

- No state and/or state actors
- Force goals by asymmetric power
- Undermine conventional mil./econ./pol. power
- Using Data-security, Privacy of the Individual

Risks/Goals

- Surprise/Shock
- Destruction
- Frustration
- Political return

„Deniability„ of Attacks



Defenders have to protect against all possible channels of attack.

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

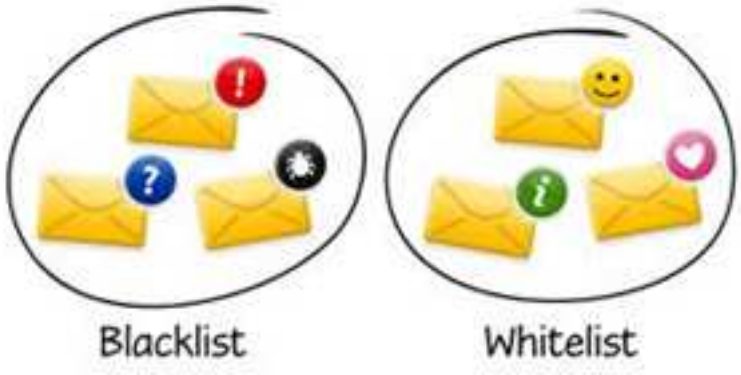
at a **time** and **place of their choice.**

→ **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, those same people you always get drunk with at PH-Neutral, HITB and CONfidence), **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 cost me a BUNCH of money!!!! ☹
- ✓ **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**. (see next slide)
- **Actors** involved may **betray you** (from all around…)
- Stay in the **white-list**.



The USS Vincennes Shot Down a Civilian Plane Because of Bad Cursors

Air Inter Flight 148 Crashed Because a Display Screen Was Too Small

Thinking AHEAD!

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

→ 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

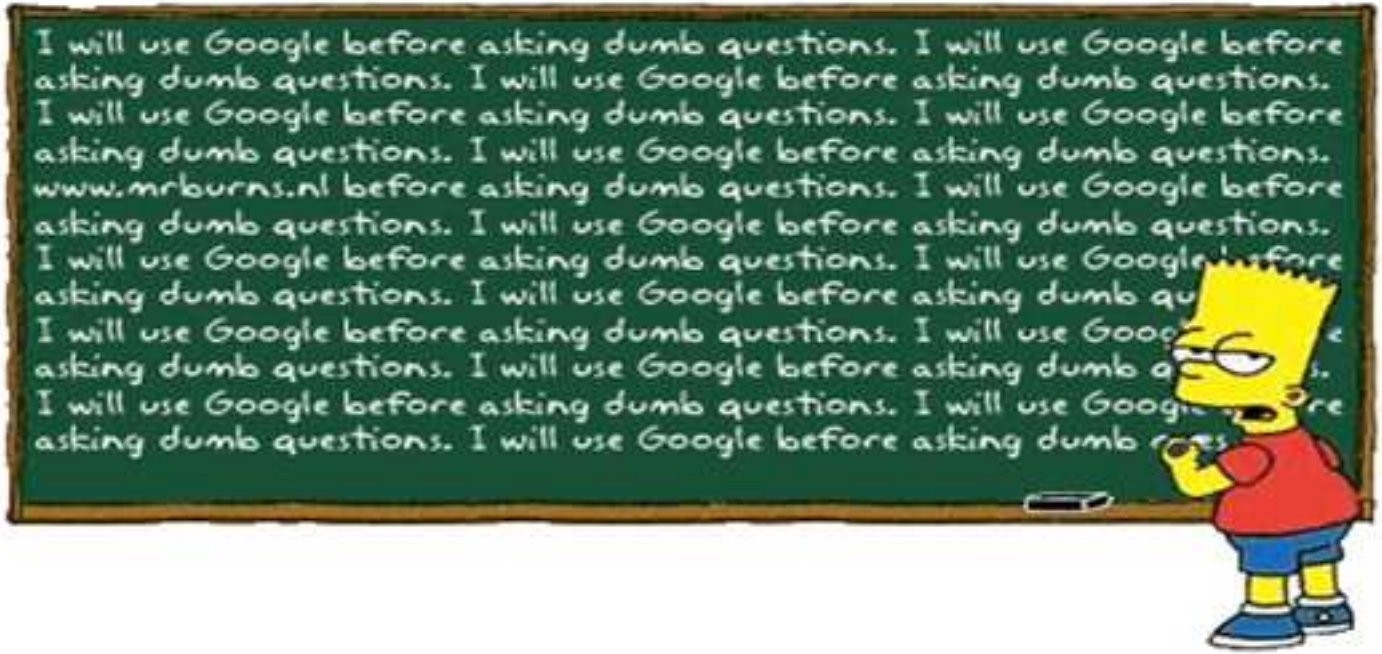
[42] http://www.enisa.europa.eu/media/news-items/enisa-teams-up-with-member-states-on-pan-european-exercise

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

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

Credits

- ❑ Advisors & Friends:
  - ✓ Jart Armin
  - ✓ Francesca Bosco
  - ✓ Alexander Klimburg
  - ✓ Indianz.ch
  - ✓ Ioan Landry
  - ✓ Naif
  - ✓ Lawyer Stefano Mele
  - ✓ Colonel Josef Schroefl, Austria MoD
  - ✓ Andrea Zapparoli Manzoni
- ❑ Supporters:
  - ✓ The Polish VODKA…
  - ✓ **And all of the CONFidence team!!!** ☺



SecurityBrokers
Global Cybersecurity Defense Services

Raoul «nobody» Chiesa

raoul@raoul.EU.org

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