Cyber Terrorism: wrong assumptions & true facts + what I hope will never happen.

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

ISACA®
Gūstot vērtību no uzticamām informācijas sistēmām
Latvijas nodaļa

Raoul «Nobody» Chiesa
President, Security Brokers

Disclaimer

- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers**, its **Associates** and **Technical Partners**.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

Agenda

- Introductions
- The real conflict: terminologies
- Cyber Terrorism
  - Definition(s)
  - The confusion
- Cyber Terrorism: the yes and the no
  - Focus: funding (money and underground digital currencies)
- Cybercrime
  - Scenarios and Actors
- Cybercrime, Information Warfare and Cyber Terrorism: the links
- Attack scenarios
  - Finance (mass spear-phishing)
  - Mobile Operators (hacking, SS7/SIGTRAN)
  - Energy Plants (SCADA, ICS)
  - Air Control Systems (ADS-B,ACARS)
  - Railways (GSM-R)
  - Naval ships (AIS)
  - E-Health (hacking)
- The WEF
- Conclusions

The Speaker

- President, Founder, **The Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Indipendent Special Senior Advisor on Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**

First of all

No common spelling…

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions…

Cybercrime is…?

No clear actors…

Cybercrime/war/terrorism ?

No common components?…

The conflict on terminologies /1

- Over the last days we've listened to **different interpretations** of «Cyber Terrorism».
- The phrase «**Cyber Terror**» appeared for the first time in the **mid-eighties**.
  - **Barry C. Collin**, a senior research fellow of the **Institute for Security and Intelligence in California**, defined Cyber Terror at that time as: the convergence of cybernetics and terrorism»: an elegant and simple definition.
  - It **wasn't enough** tough, to make clear distiction with terms like **Cybercrime**, **Cyber Activism** (Hacktivism) and **Cyber Extremism**.
- Back in **1997**, Mark **Pollit from the FBI** defined Cyber Terrorism as:

The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents (FBI, 1997).

- In **2004**, **FBI** redefined the term of Cyber Terrorism as (Lourdeau, 2004):

A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda (FBI, 2004).

The conflict on terminologies /2

- In **2002**, the **US Center for Strategic and International Studies** defined Cyber Terrorism as:

The use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population (Lewis, 2002).

- The **UK Terrorism Act** goes further:

The use or threat of action designed to influence the government or an international governmental organisation or to intimidate the public, or a section of the public; made for the purposes of advancing a political, religious, racial or ideological cause.

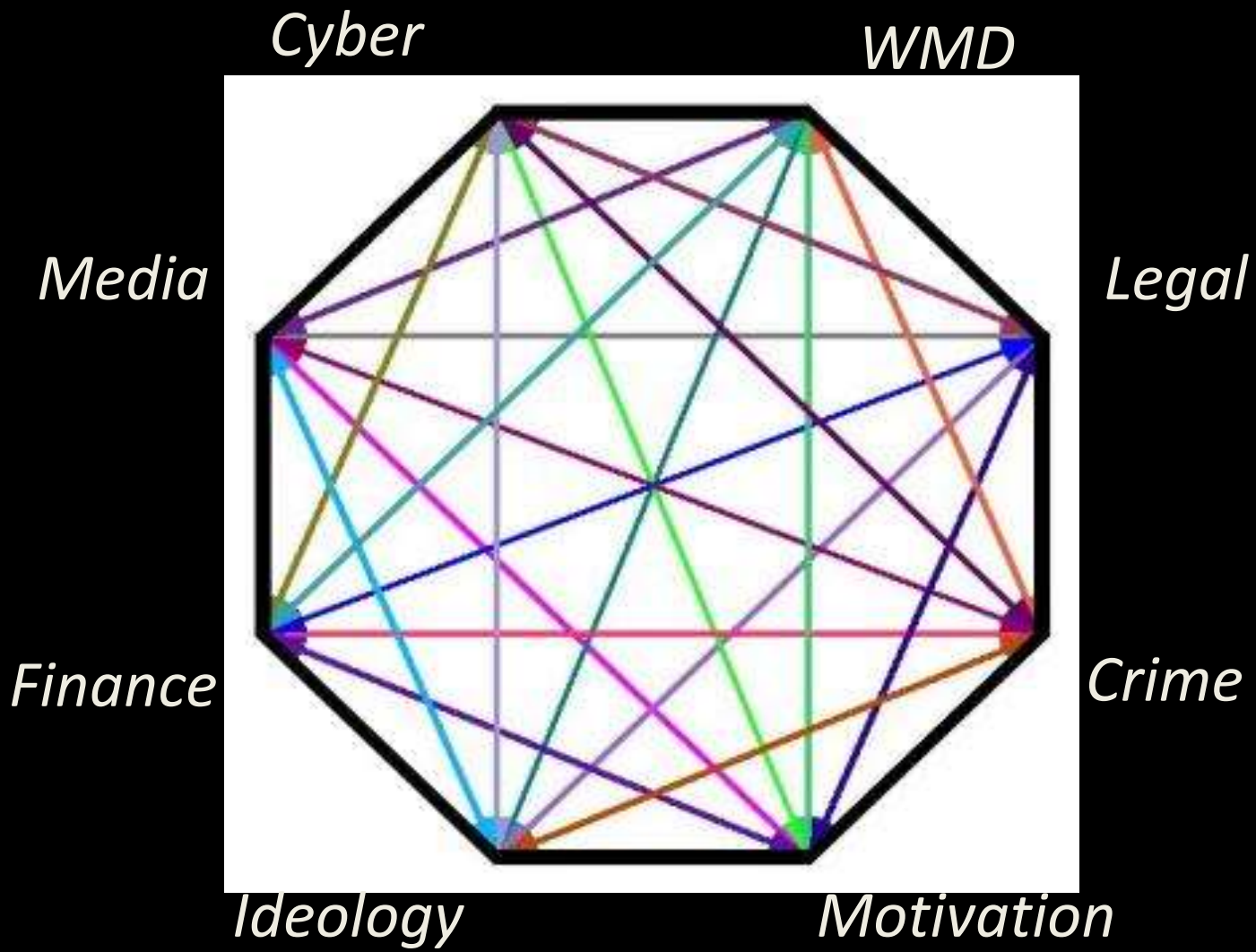
It involves or causes:

- *serious violence against a person;*
- *serious damage to a property;*
- *a threat to a person's life;*
- *a serious risk to the health and safety of the public; or*
- *serious interference with or disruption to an electronic system (UK Terrorism Act 2000).*

The conflict on terminologies /3

- No **commonly agreed definition** of *terrorism* (!)
- **International** Acts and treaties;
  - UN Resolutions 1368&1373
  - NAC decision dated 03 Oct 2001
  - EU Counter-Terrorism strategy
- Terrorist Organizations **lists** (even if… see later)
- International Law Authorities: **Enough tools** for combatting terrorism?
- Political will of **all nations**

Dimension of modern, global terrorism



Don’t miss different perspexctives!

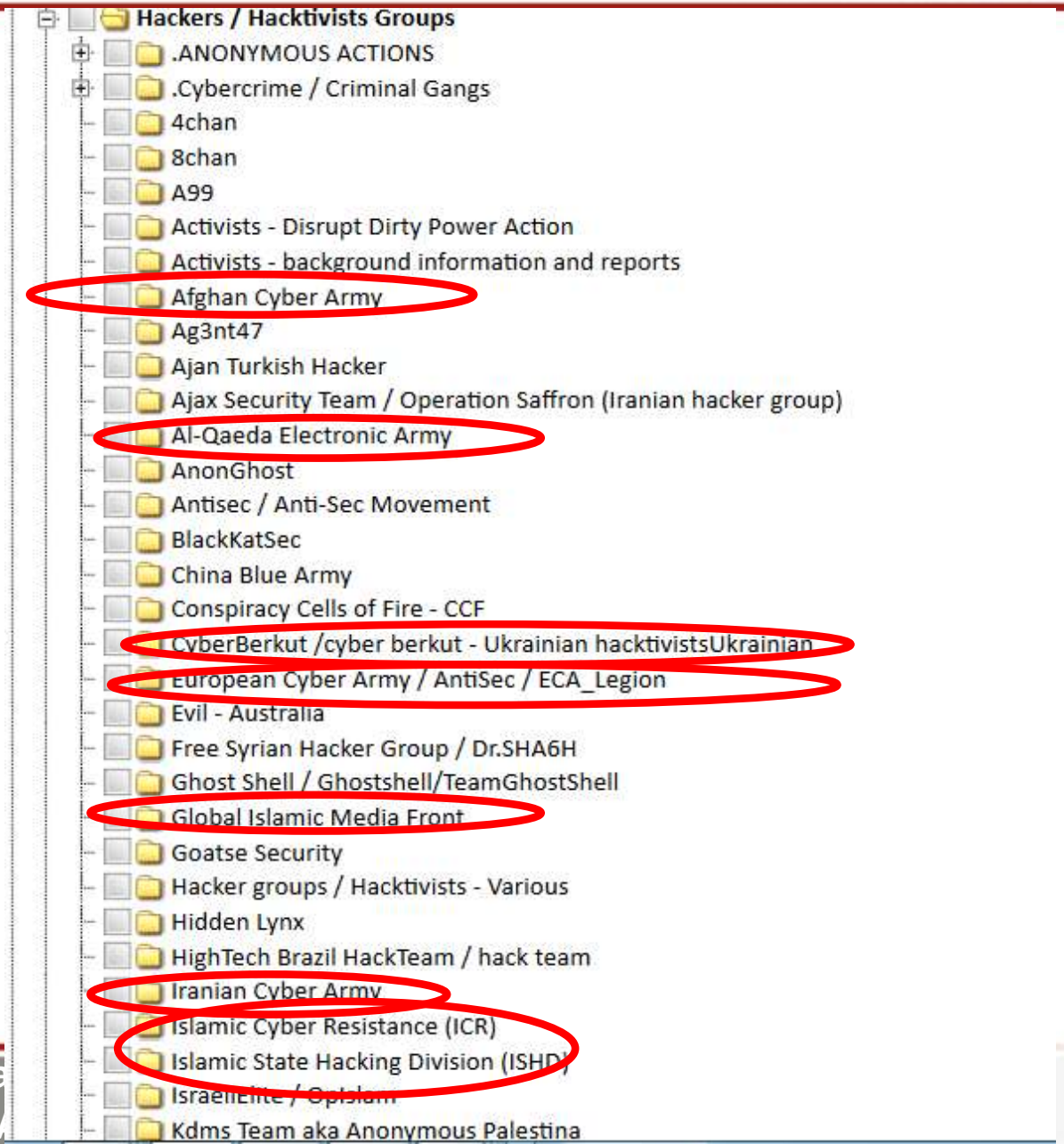
- Has a **Cyberterrorism attack** already happened?
  - **NO** (thanks God!)
- As of today, terrorist organizations make use of the Internet in order to:
  - **Publicity/Advertising and Propaganda**
  - Data Mining
  - Recruiting and Mobilization
  - **Fundraising**
  - Networking / Sharing Information
  - Training
  - Planning and Coordination
  - Claiming attack’s responsability, showing «what they have been able to do»
- The point is that they may make much worse, if they would know **how to make it**.
  - We’ll speak about this later.

Making propaganda

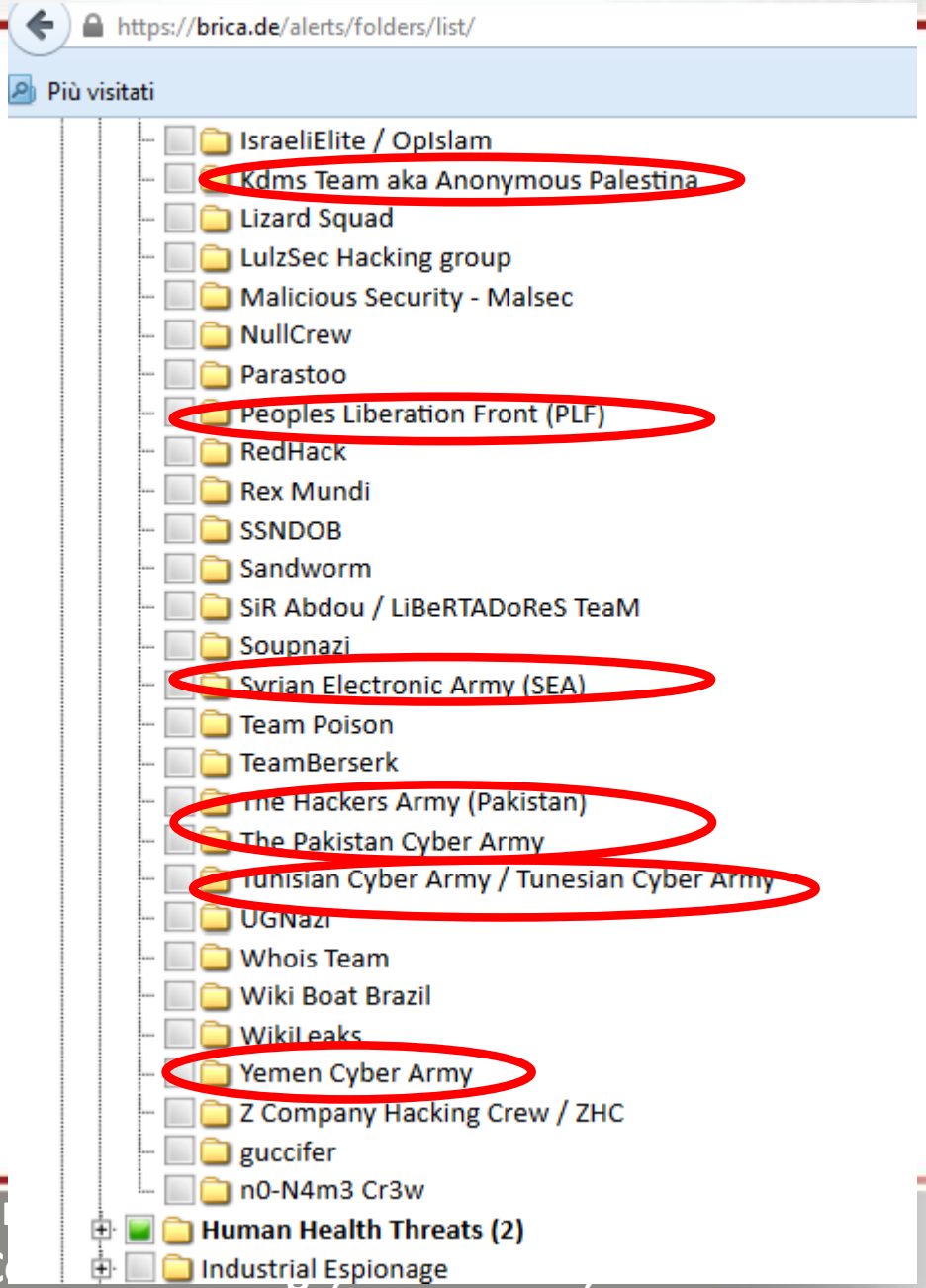
- Terrorism / Govt Intelligence (8)
  - . Specific Terrorist Groups (5)
    - Abu Sayyaf
    - Ajnad Misr/Soldiers of Egypt
    - Ajnad al-Sham
    - **Al Qaeda/al-Qaida /Al Queda / AQIM/AQAP/AQSL**
    - Al-Murabitoon
    - Al-Qassam / Al-Qassam
    - Al-Shabaab / Al Shabaab / al-Shabab
    - Ansar Bayt al-Maqdis
    - As-Sahab
    - Boko Haram
    - Cyber Caliphate / CyberCaliphate
    - Hezbollah
    - Hizb-ut-Tahrir / HTA (Hizb ut-tahrir America)
    - Houthi militants / Houthi group / Houthi rebel
    - **IS /ISIS/Islamic State/ISIL/Takfiris/AQI/ Daish/ Daesh**
    - Jabhat al-Nusra
    - Jaysh al-Islam
    - Jund al-Khilafa
    - Khorasan
    - Specific Terrorist Groups - Various
    - Tehreek-e-Taliban / Taliban
  - **. Inspire / Azan / Dabiq Terrorist Magazines**
  - **. Terrorist / Govt Intel Alert**
  - .Terrorist / Govt Intel Background reports and Info
  - .Terrorist / Govt Intel News
  - Green Dam
  - Kylin

Remaining subjects for your subscription	99
Global	**100**
Activated subjects	19
Remaining subjects for your subscription	81
Organization	**10**
Activated Search terms	0
Remaining search terms for your subscription	10

Hackers, Hacktivists = Cyber Terrorists?



Hackers, Hacktivists = Cyber Terrorists?



Funding: «Cyber Hawala?

You probably know about “HAWALA”

Hawala (also known as hundi) is an informal value transfer system based on the performance and honour of a huge network of money brokers

Learning from terrorism financial models

Many of electronic payment systems are following the HAWALA principle
And built on the top of similar infrastructure

Now backed by digital inftastructure

No traces in banking network

Money disappear in one place, pop up in another

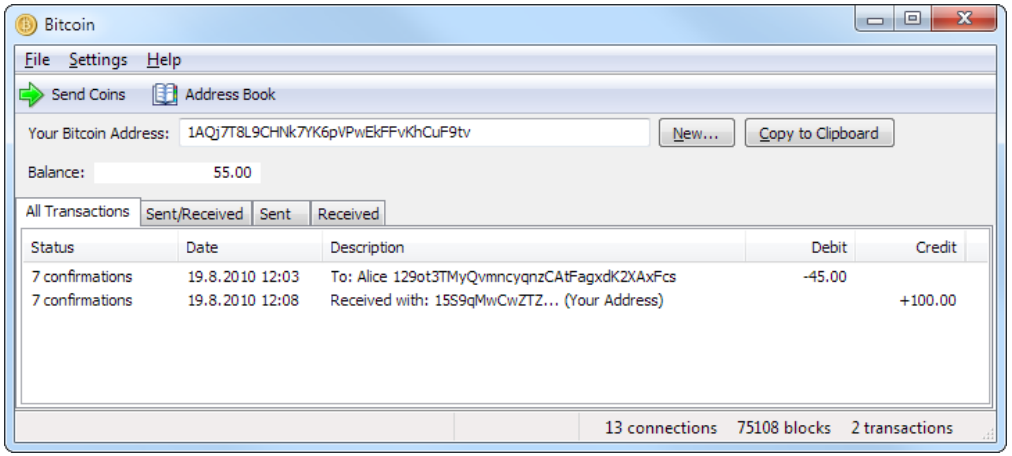
Underground currencies

Lets look at some examples

There is more than one way to transfer money

Digital currencies

- Don’t think just about **bitcoins**!



"Underground" currencies

Getting to know "Underground" money systems

- WMZ - web money - one wmz = one USD
- Drop - money mule
- CC - creditcards
- Abuse resistant - Safe to host any kind of fraudulent service
- Partnerka - partnership program

WMR – эквивалент RUB
WMZ – эквивалент USD
WME – эквивалент EUR
WMU – эквивалент UAH
WMB – эквивалент BYR
WMY – эквивалент UZS
WMG – эквивалент 1GG

“Underground” currencies

There are many:

- Web Money (WMZ)
- Yandex Money
- LR (liberty reserve
- Epassporte (dead!)

Where is webmoney office in Thailand?

Webmoney Gate Czech	Прага	Чехия
Webmoney в Брянске	Брянск	Россия
WebMoney Club	Орел	Россия
WmPerm.RU	Пермь	Россия
wmTrader.BIZ	ОМСК	Россия
WMCashing	Санкт-Петербург	Россия
WebMoney центр в Великобритании	Нортхэмптон	Великобритания
oWMT.ru - Генеральный дилер Webmoney Transfer	ОМСК	Россия
Webmoney.kg	Бишкек	Кыргызстан
WMT-Tula, сервис WebMoney в г. Тула	Тула	Россия
Moscow Transfer	Москва	Россия
WMZ.lv	Рига	Латвия
Webmoney Israel	Хадера	Израиль
WebMoney Exchange Point, Pattaya, Thailand	Патайя	Тайланд
Финансовый цен		
Ростовский обме		
Webmoney24	Санкт-Петербург	Россия
Обменный пункт Webmoney в Екатеринбурге	Екатеринбург	Россия
E-money - электронные деньги в Кыргызстане	Бишкек	Кыргызстан

Pataya!! Where gangsters are ;-)

“Underground” currencies

Credit card “dumps” websites, work only with “trusted” systems. Why?

AlertPay, SMS, LiqPay

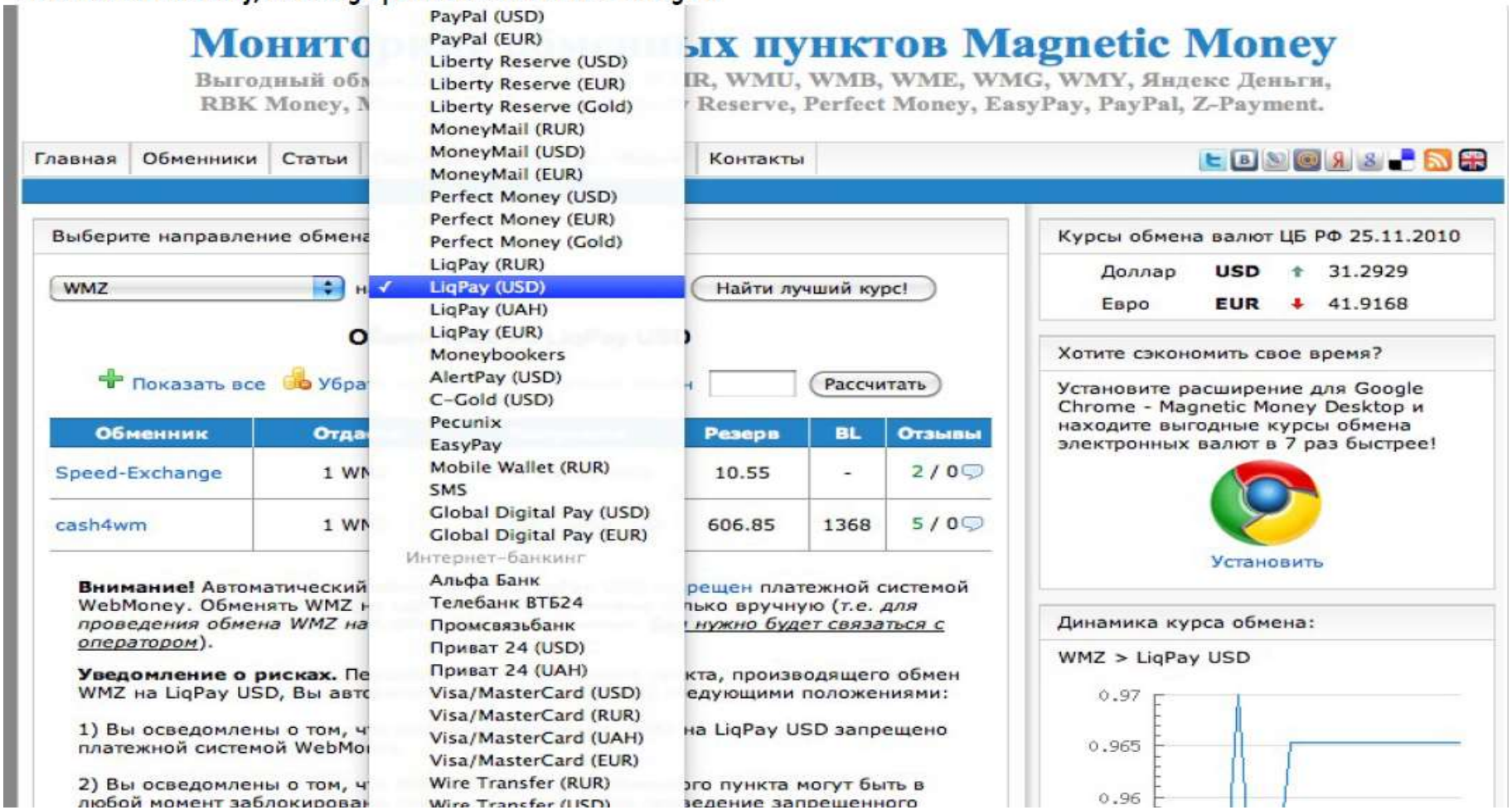
"Underground" currencies

They feature "awesome" geographical locations

Liberty Reserve – largest payment processor and money transfer ... +1 -
www.libertyreserve.com/ - 頁庫存檔
Oldest, safest and most popular payment processor operating in Costa Rica and serving millions all around a world. Store your funds privately in gold, Euro or ...

“Underground” currencies

As with real currency, exchange points exist. Percent charged:



The scenario(s) and the Actors

Crime -> Today

*You got the **information**, you got the **power**..*

Simply put, this happens because the "*information*" can be **transformed at once** into "something else":

1. **Competitive advantage (geo/political, business, personal relationships)**
2. **Sensible/critical information (blackmailing, extorsion)**
3. **Money (Cash-out techniques, Black Market & Underground Economy)**

- … **that's why** all of us we want to "*be secure*".

- It's not by chance that it's named "IS": **Information Security** ☺
  - The **trend** of the «*cyber-prefix*» is from **very recent years**, tough.

Cybercrime

- **Cybercrime**:

  *"The use of IT tools and telecommunication networks in order to **commit crimes** in **different manners**".*

- **The axiom of the whole model:**

  *"acquiring different types of **data** (information), which can be transformed into **an advantage**."*

- **Key points**:
  - **Virtual** (pyramidal approach, anonimity, C&C, flexible and scalable, moving quickly and rebuilding fast, use of "cross" products and services in different scenarios and different business models)
  - **Transnational**
  - Multi-market (**buyers**)
  - **Differentiating** products and services
  - **Low** "entry-fee"
  - **ROI** /Return of Investment (on each single operation, which means that, exponentially, it can be industrialized)
  - Tax & (cyber) Law **heaven**

Why?

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

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

"2013 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

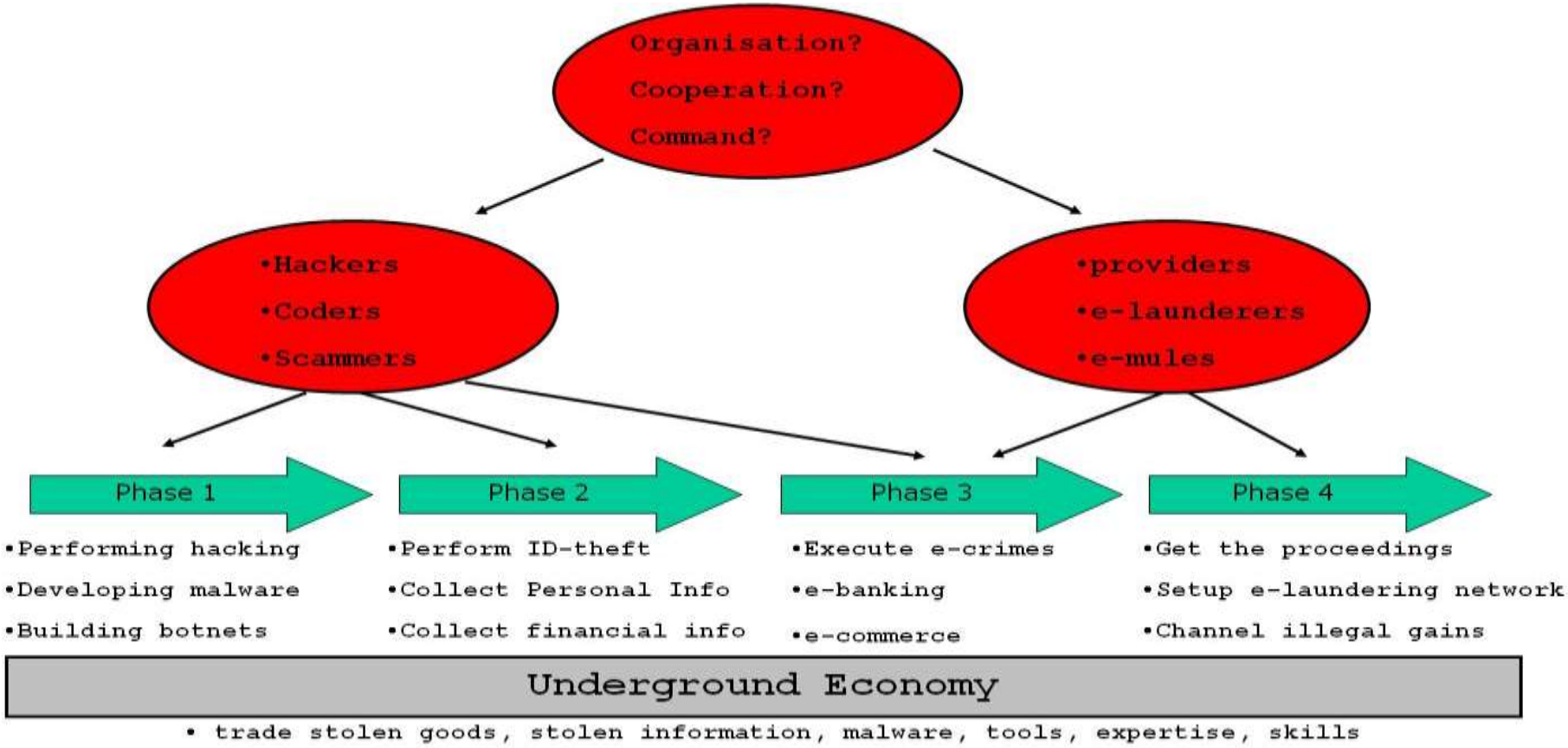
Various sources (UN, USDOJ, INTERPOL, 2013)

Financial Turnover, estimation: 12-18 BLN USD$/year

From Cybercrime to…

- We are speaking about an ecosystem **which is very often underevaluated**: most of times, Cybercrime is the **starting** or **transit point** towards different ecosystems:
  - **Information Warfare**
  - **Black Ops**
  - **Cyber Espionage**
  - Hacktivism
  - (private) **Cyber Armies**
  - **Cyber Terrorism (?)**
  - Underground Economy and Black Markets
    - Organized Crime
    - Carders
    - Botnet owners
    - 0days
    - Malware factories (APTs, code writing outsourcing)
    - Lonely wolves
    - "cyber"-Mercenaries

Cybercrime MO



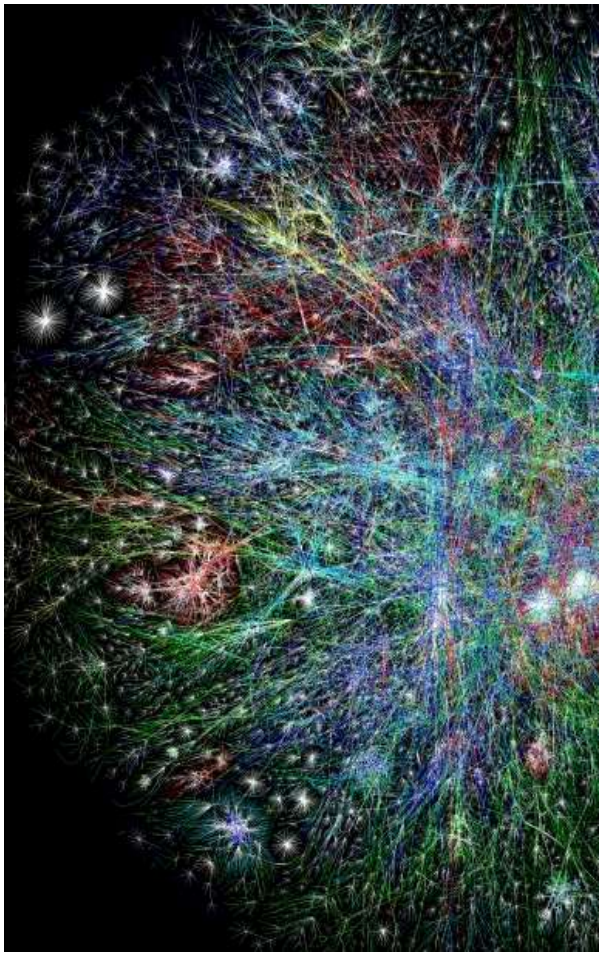
Profiling Actors

New Actors joined in

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

- **All of the above is launched against any kind of targets:** Critical Infrastructures, Governative Systems, Military Systems, Private Companies of any kind, Banks, Medias, Interest Groups, Private Citizens....
  - National States
  - IC / LEAs
  - Organized Cybercrime
  - Hacktivists
  - Industrial Spies
  - **Terrorists**
  - Corporations
  - Cyber Mercenaries

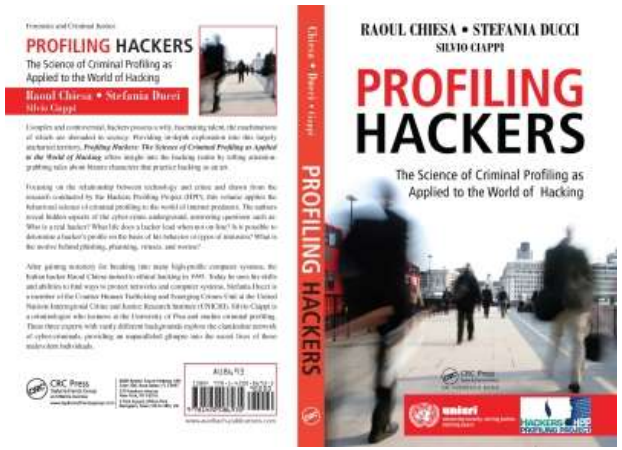
Everyone against everybody



Welcome to HPP!

HPP V1.0

- Back in **2004** we launched the Hacker's Profiling Project - HPP: http://www.unicri.it/special_topics/cyber_threats/
- Since that year:
  - **+1.200 questionnaires** collected & analyzed
  - **9 Hackers profiles** emerged
  - **Two books** (one in English)
    - Profilo Hacker, Apogeo, 2007
    - Profiling Hackers: the Science of Criminal Profiling as Applied to the World of Hacking, Taylor&Francis Group, CRC Press (2009)



unicri
advancing security, serving justice, building peace

	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

PROFILE	MAY BE LINKED TO	WILL CHANGE ITS BEHAVIOR?	TARGET	(NEW) MOTIVATIONS & PURPOSES
Wanna Be Lamer		No		
Script Kiddie	Urban hacks	No	Wireless Networks, Internet Café, neighborhood, etc..	
Cracker	Phishing Spam Black ops	Yes	Companies, associations, whatever	Money, Fame, Politics, Religion, etc…
Ethical Hacker	Black ops	Probably	Competitors (Telecom Italia Affair), end-users	Big money
Quiet, Paranoid, Skilled Hacker	Black ops	Yes	High-level targets	Hesoteric request (i.e., hack "Thuraya" for us)
Cyber-Warrior	CNIs attacks Gov. attacks	Yes	"Symbols": from Dali Lama to UN, passing through CNIs and business companies	Intelligence ?
Industrial Spy		Yes	Business company / Corporation	For profit
Government Agent		Probably	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker		Probably	Government / Strategic company	Monitoring / controlling / crashing systems

HPP V2.0: what happened?

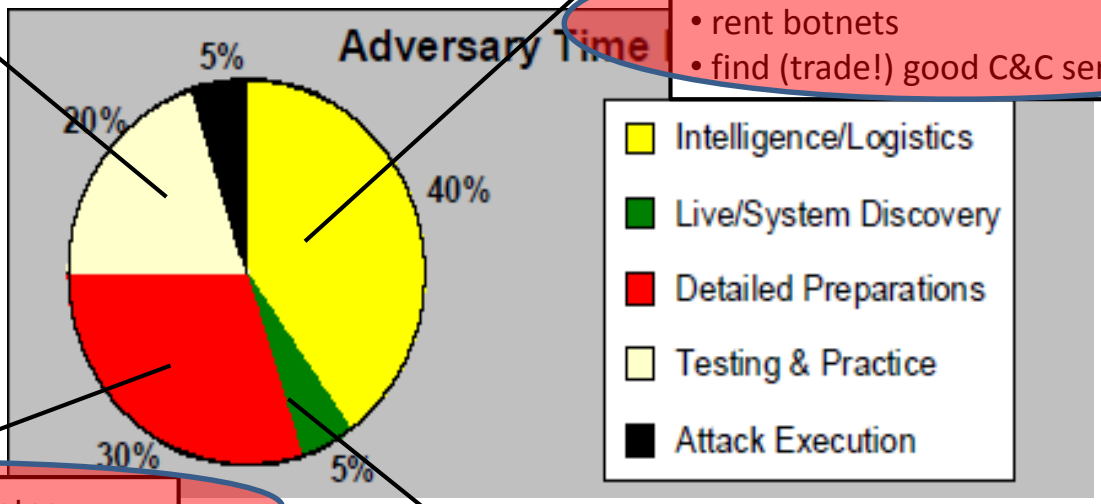
- VERY **simple**:
- **Lack of funding**: for phases 3&4 we need support!
  - HW, SW, Analysts, Translators
- We started back in **2004**: «romantic hackers», + we foreseen those «new» actors tough: **.GOV**, **.MIL, Intelligence.**
- We **missed out**:
  - Hacktivism (!);
  - Cybercriminals out of the «hobbystic» approach;
  - OC;
  - The financial aspects (Follow the Money!!);
  - **Cyberterrorists** (do they really exist?)

unicri
advancing security, serving justice, building peace

Making "Cyber War"…

- equipment to mimic target network
- dummy run on similar network
- sandbox zerodays

- „dummy list" of „ID-10T" for phishing
- background info on organisation (orgchart etc.)
- Primer for sector-specific social-engineering
- proxy servers
- banking arrangements
- purchase attack-kits
- rent botnets
- find (trade!) good C&C server



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

Alexander Klimburg 2012

- Purchase L2/L3 system data

«Attack attribution»

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

Major General Keith B. Alexander,
Commander US CYBERCOM / NSA, testimony May 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**

Source: Alexander Klimburg, 2012

Mistyping may lead to (very) different scenarios…

Non-state proxies and "inadvertent Cyberwar":

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

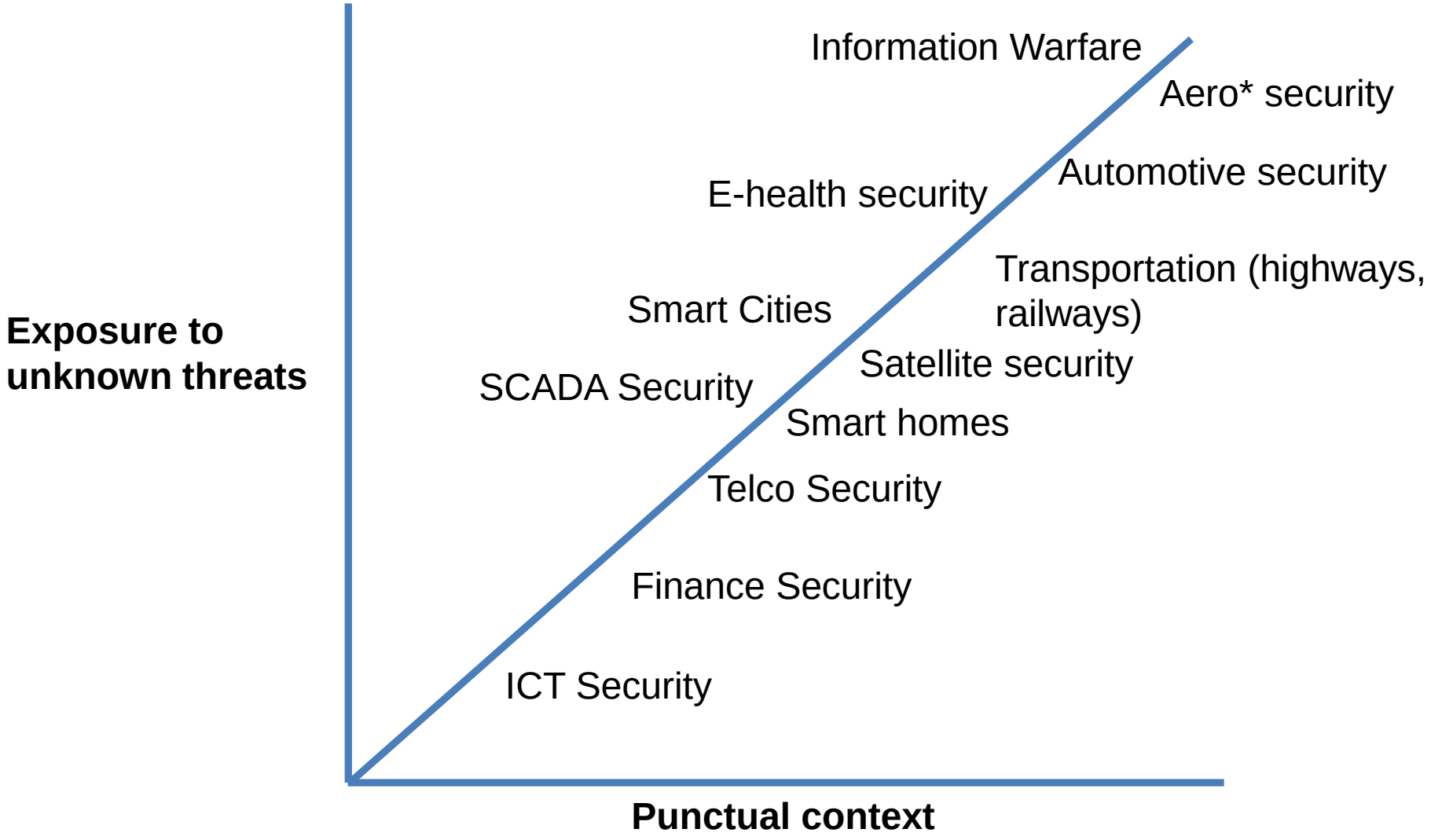
How does country B know if:

a) *The attack is conducted with consent of Country A (**Cyberwar**)*

b) *The attack is conducted by the proxy network itself without consent of Country A (**Cyberterrorism**)*

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

What if….


Information Warfare
Aero* security
Automotive security
E-health security
Transportation (highways, railways)
Smart Cities
Satellite security
SCADA Security
Smart homes
Telco Security
Finance Security
ICT Security
Exposure to unknown threats
Punctual context

IT and ICT attacks… (currently available!)

… WHICH COULD BE USED BY TERRORIST ORGANIZATIONS

- Giving all what we said, it's definitely **clear and easy to understand** how much **IT and ICT based attacks may impact on a Nation State**.
- During our research studies we encountered many **different, concrete evidences** of already-existing **knowledge**, developed by **Security Researchers** and **Ethical Hackers**.
- As you have seen during my presentation, we have decided **not to focus** yet on those extremely technical details, while instead providing a first, **big picture** and general view on the **Cyber Terrorism topic**.
- Nevertheless, we want to **point out some of those apparently niche knowledge** we have scouted, studied and analyzed, thus applying them to a **possible, global attack on a target country**, which **terrorists may already carry on now**, since the **needed information are, more or less, publicly available**.

What's at stake?

Among all of our findings and **theoretical attack scenarios**, we focused on the following ones:

- **SCADA and Industrial Automation**.
- **Finance Sector:** ATMs
- **Transportation, Avionics:** ADS-B and ACARS
- **Transportation, Marine:** AIS.
- **Transportation, Automotive.**
- **Transportation, Highways, Railways.**
- **Public Safety:** IP-based CCTVs.
- **Personal Privacy:** Smart TVs.

- Much more could be add to this selection, giving the fact that actual and emerging technologies, as a matter of fact, do not came with the so-called "**Security by Design**" approach, which brings an **amazing amount of vulnerabilities**, which do impact, in a **domino effect**, to **different environments**, allowing **never-seen before attack scenarios**.

Aircraft Security

- The (ethical) hacking community discovered this long time ago
  - Hugo Teso (DE) – we'll see on next slides
  - Renderman (CA)
  - Ruben Santamarta (ES)
  - Myself (IT)
  - More security researchers

+

Hackers + Airplanes

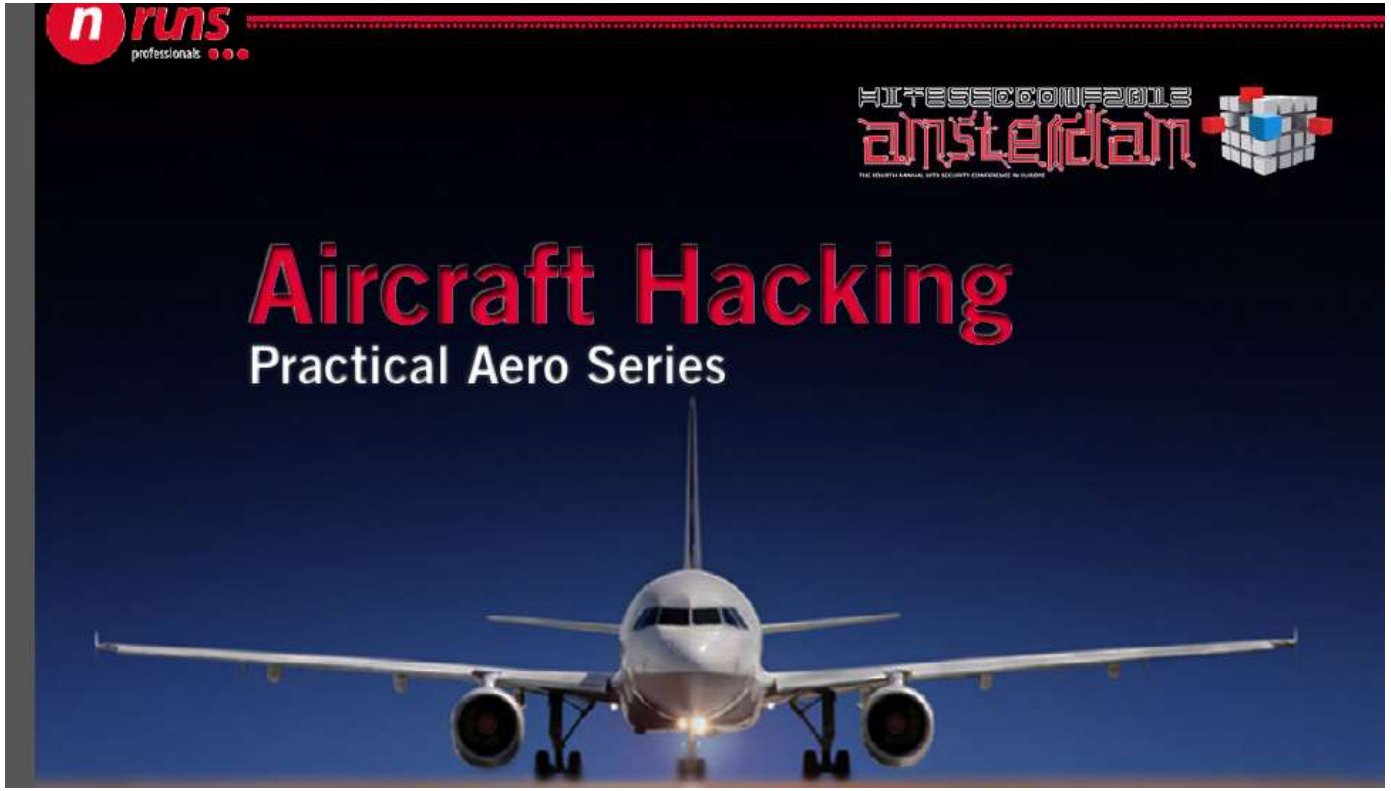
No Good Can Come Of This

Confidence 2012
Brad "RenderMan" Haines, CISSP
www.renderlab.net
render@renderlab.net
Twitter: @IhackedWhat

=

Air Traffic Control Security

- Back in **2013**, I was attending a presentation at **Hack in the Box** in Amsterdam by Hugo Teso



Air Traffic Control Security

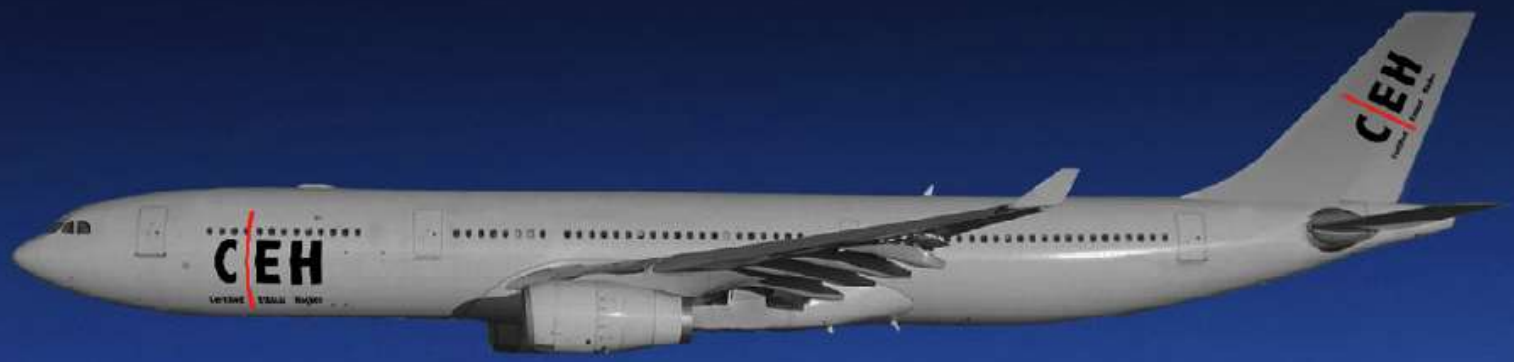
Attack Overview

DISCOVERY:
» ADS-B

INFO GATHERING:
» ACARS

EXPLOITATION:
» Via ACARS
» Against on-board systems vulns.

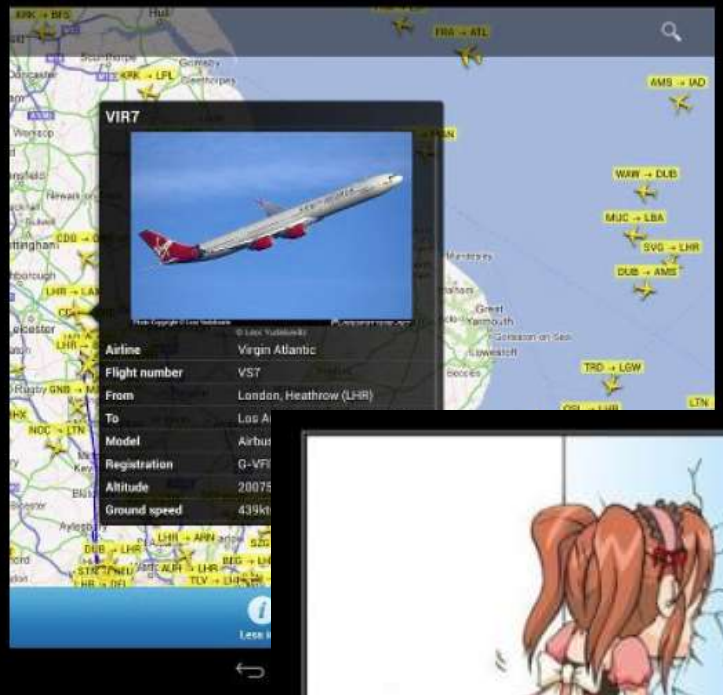
POST-EXPLOITATION:
» Party hard!



Air Traffic Control Security (ADS-B)

ADS-B 101

- Automatic Dependent Surveillance-Broadcast
- Radar substitute
- *Position*, *velocity*, *identification*, and other ATC/ATM-related information.
- ADS-B has a data rate of 1 Mbit/sec.
- Used for locating and plotting targets



FACEWALL

WHEN A FACEPALM IS NOT ENOUGH

ADS-B Security

- None at all
- Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying, injection).
- Target selection
  - » Public Data
  - » Local data (SDR*)
  - » Virtual Aircrafts

* Software Defined Radio

Air Traffic Control Security (ACARS)

ACARS 101

- Aircraft Communications Addressing and Reporting System
- Digital datalink for **transmission of messages between aircraft and ground stations**
- Multiple data can be sent from the ground to the A/C *
- Used for passive "OS fingerprinting" and plotting targets

ACARS Security

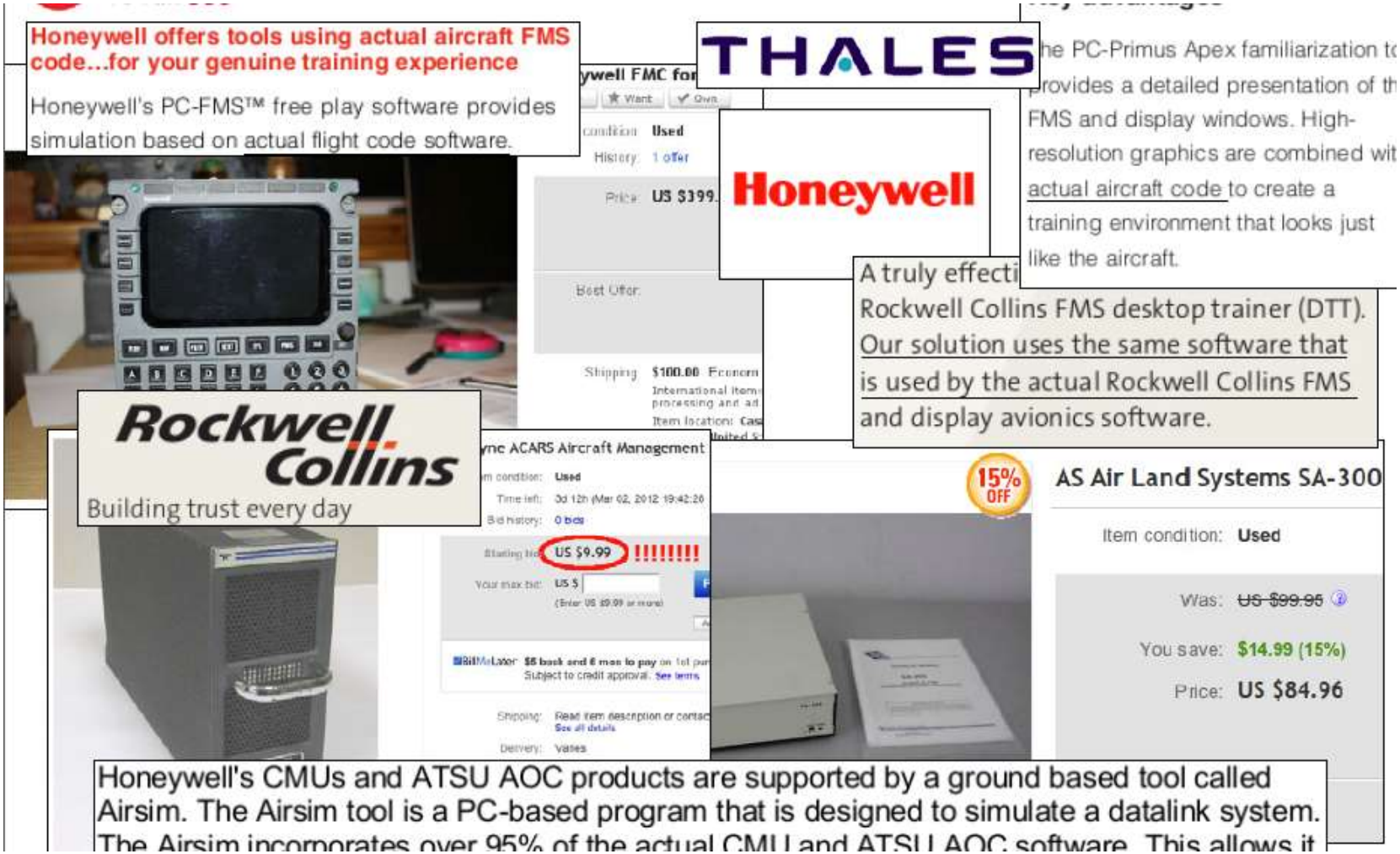
- None at all
  - » sometimes monoalphabetic ciphers
- Detailed flight and Aircraft information
  - » Public DB
  - » Local data (SDR)
  - » Virtual Aircrafts
- Ground Service Providers
  - » Two main players
  - » Worldwide coverage

Air Traffic Control Security (FMS)

Air Traffic Control Security (FMS)

Air Traffic Control Security (FMS)

Air Traffic Control Security (FMS)

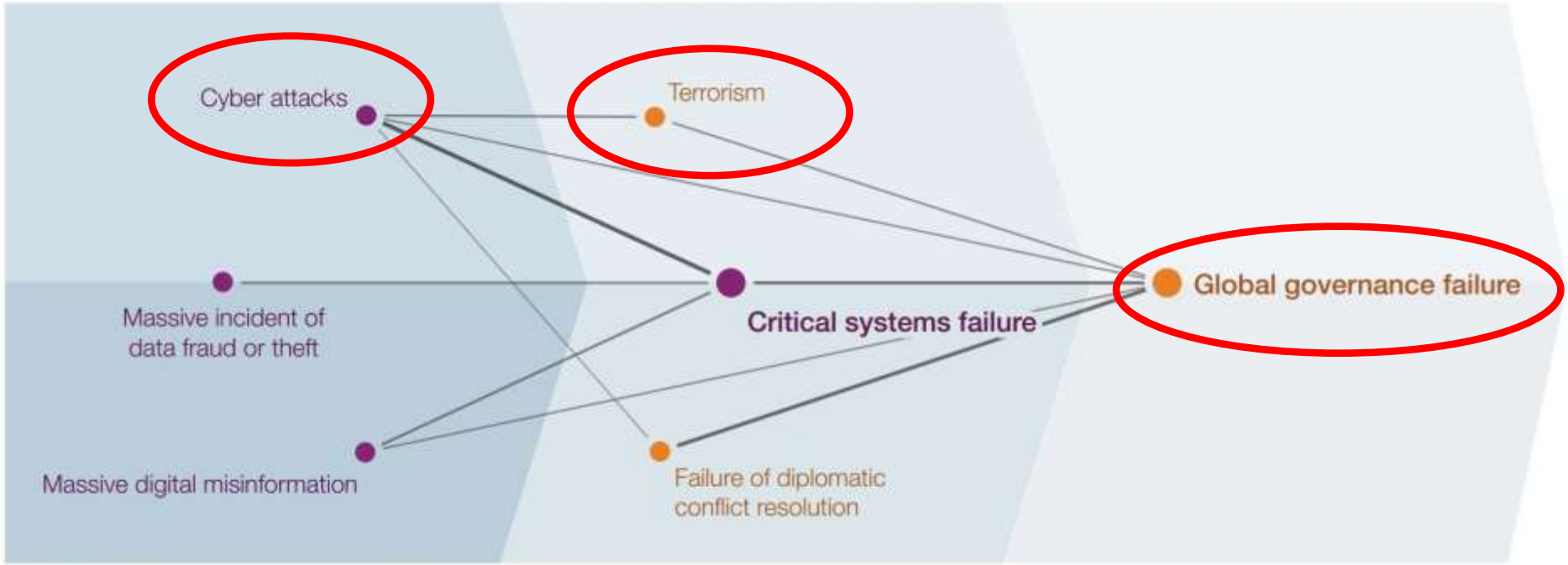


World Economic Forum

Figure 38: Technological Risks

World Economic Forum

Figure 17: The Dark Side of Connectivity Constellation



Origin Risk
Increasing capabilities for cyber crime and attacks.

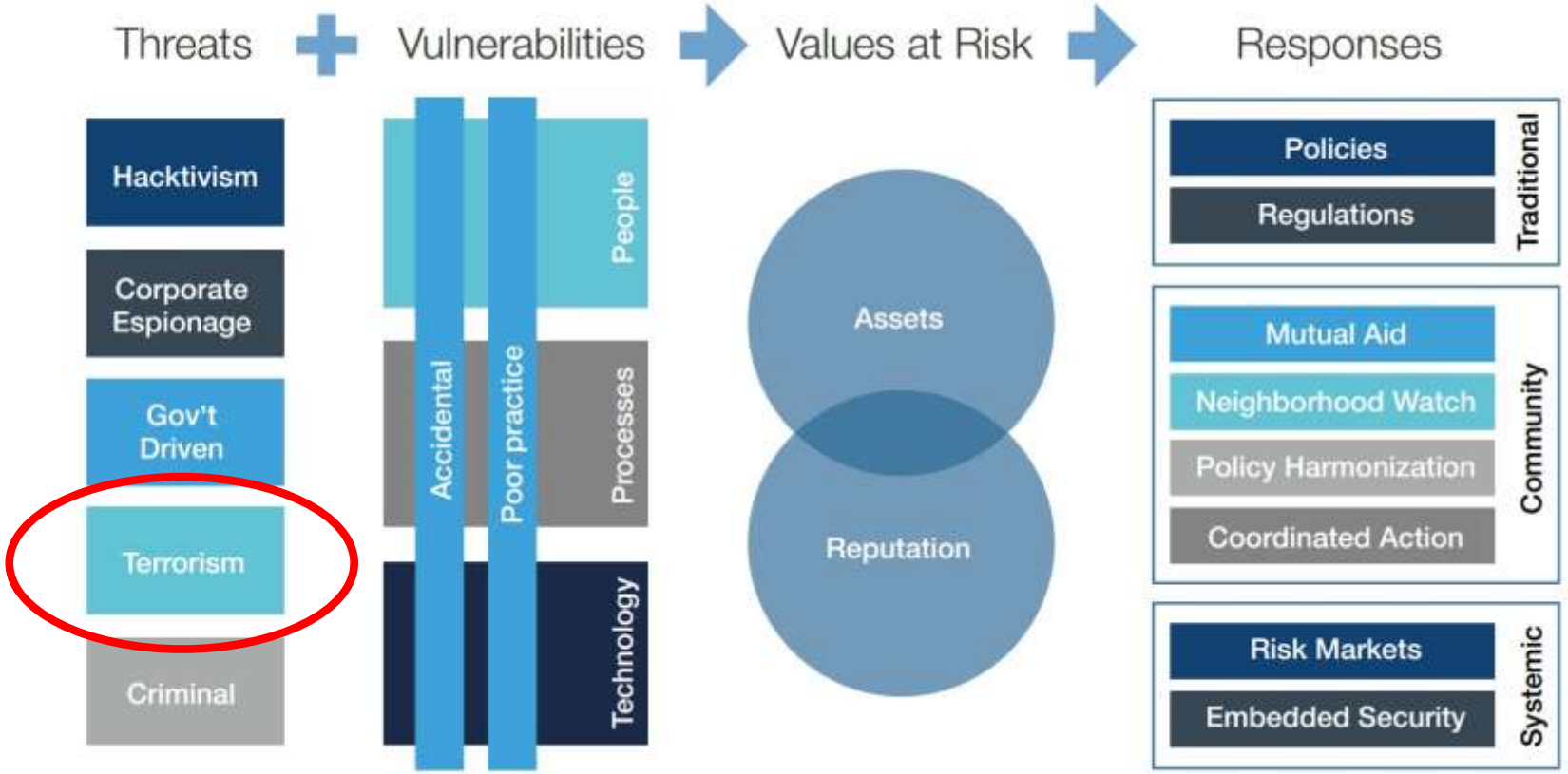
Pathways
Balance-of-power tips as new actors can wage effective interference and disrupt commerce.

Manifestation
The traditional system of global governance is undermined.

Source: World Economic Forum

World Economic Forum

Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum

Hackmageddon

- We think it is clear enough how the industry, manufacturers and system integrators, as well as Governments and Policy Makers, must **immediately take actions in order to avoid that** different, unconventional and unexpected scenarios **became a reality**.

- Giving all the above, we may draw a final, **overall scenario**, on which the following attacks may be carried out by single or multiple **terrorist organizations**, acting both individually or in a **coordinated and concerted attack plan**.

This must not happen. Ever.

- **6AM, Monday**: massive fire in the national oil and gas platforms all over the Country X coast. The incident is suspected to be the result of malfunction in the control systems of platforms.

- **8AM, Monday**: the late rescue operations suffer from big chaos and lack of coordination, as a result of unexpected breakdowns in the communication networks belonging to the security forces and civil defense.

- **8PM, Monday**: hot news appears on the prime time news at national and international TV channels. The collision of two air planes over the international airport at Country X capital looks like the result of a sophisticated Air Traffic Control cyberattack launched against the communications between the two involved planes and the flight control tower of the airport itself. The initial reports were speaking about an "unknown jamming source" on the radar and navigation systems of the international airport.

This must not happen. Ever.

- **On Tuesday morning**, all ATM machines are out of service in various areas of the country, due the to collapse of the internal networks and the main servers of Country X banks. Cybersecurity experts say that the ATMs were infected with a tailored worm, which disabled all of ATM's functionalities.

- **Later in the afternoon**, random ATMs were reported to throw out cash, in the form of 10, 20, 50 and 100 Country X local currency (bills). Riots were reported in different areas of the involved cities, as well as urban guerrillas between Law Enforcement Officers and citizens.

- **On Tuesday afternoon**, all of CCTV cameras installed in the capital city went out of order: Law Enforcement Agencies cannot monitor anymore the situation in the streets and public safety is at risk.

This must not happen. Ever.

- **On Tuesday night**, the navigation control infrastructure for ships ran by the Navy Control Authority reported multiple problems, ranging from ships suddenly disappearing from the radars to hi-jacked position of known ships, and unknown ships popping up on the radars themselves. Civilian and Military naval control systems literally went blind and can't be considered reliable anymore.

- **On Wednesday**, cut off of all communications means in the country, especially the cellular and fixed telephone networks; the news are confirmed, Country X is under a massive, violent cyberattack, for which the terrorist organization "ABC" claimed to be responsible, and the cyber group "Souls of Allah" the executors. All of the vital sectors of Country X can't be considered reliable, and citizens are asked to not leave their homes. Schools and Universities, as well as Public Offices, have been closed for security reasons.

- **On Thursday**, multiple citizens suffered apparently poisoning from public water and needed urgent medical help. The hospital of main cities of Country X reported more than 3000 injured people. Security experts reported SCADA attacks to the Water Systems of five different cities.

This must not happen. Ever.

- **7PM, Saturday**: the whole country is without electrical energy. Massive and distributed cyberattacks to the National Electric Grid have been reported. The national energy company can't grant anymore the delivery of electricity for most than 75% of the whole country; electricity power groups and UPS systems will end their self-power capacity by 3 to 6 hours.

- **5AM, Sunday**: more than 30.000 soldiers from the terrorist group "ABC" invaded Country X. Disorders, murders, violence and rapes are reported in all of the main cities and small towns of the country. The Prime Minister has been assassinated and the Parliament has been assaulted; right now the military forces are fighting battles with the terrorist troops in many district of the capital; robberies rise up and the situation is close to a state of Civil War. National security is not granted anymore and the overall stability of Country X is at risk. Citizens are escaping from the country, crossing borders by all possible means and entering in Country B and Country C as "war refugees".

Conclusions

- **Everything has changed**. We are sitting on a **fully unstable chair**. This field of research is **totally new to everyone**. Too much stuff is just **too much underevaluated** here.
- The technologies and environments we are speaking about, which automatically lead to different types of combined, **asymmetric Cyber Attacks**, if **designed and weaponized into a single, distributed attack framework**, would cause significant impacts, disruptions and public panic in a given **target country**.
- What we are speaking about it's not **Hollywood**, while definitely it could lead to 1982 **Wargames movie** and that famous «Global Termo Nuclear War»
- **Critical Infrastructures** play a **critical role** here.
- Ask for technical solutions from the Security Industry, be compliant with security standards and regulations, but **don't forget both taking from and giving back to the security communities**.

Contacts, Q&A

- **Need** anything, got **doubts**, wanna **ask me smth**?
  - rc [at] security-brokers [dot] com
  - Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?