

KEYNOTE (itinerante :) 4 CyberSec topics VS 4 InfoSec Cultures

Raoul “Nobody” Chiesa Ing. Selene Giupponi

Cyber Security
PARMA



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 local National laws.
- The information contained in this presentation is for **educational purposes** and **knowledge information** only; the authors **are not responsible** if you will use this material in order to **damage people, assets, things**.
- The authors hold the **intellectual property** and **it's not allowed to use this material for different purposes**.
- The Hackers Profiling Project is hold by **UNICRI** and **ISECOM** and was **created by Mr. Raoul Chiesa**.
- 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** and **its own Associated Partners and Companies**.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information, and authorship, is acknowledged, mentioned and credited**.

Agenda

- * Introductions
- * Terminologies...
- * The real world
 - * Actors
- * 4 Cultures, 4 Topics (PART I)
 - * Asset as a concept
 - * Automotive, Ransomwares, DNS Exfil, Ethical attacks
- * Conclusions





Introductions

unipr# whois Raoul

- President, Founder, **The Security Brokers**
- Independent Special Senior Advisor on Cybercrime @ **UNICRI**
(United Nations Interregional Crime & Justice Research Institute)
- Roster of Experts @ **ITU** (UN International Telecommunication Union)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, Former Member @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI** (Privacy & Security Observatory)
- Board of Directors, **ISECOM** (Institute for Security & Open Methodologies)
- **OSSTMM** Key Contributor (Open Source Security Testing Methodology Manual)
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè. Scientific Committee, **APWG** European Chapter
- Former Board Member, **AIIC** (Italian Association of Critical Infrastructures)
- **Supporter at various security communities**



unipr# whois Selene

- * **Managing Director Europe, RESecurity**
- * **Computer Engineering Degree + II Level Master in Computer Forensics & Digital Investigations**
- * General Secretary and Member @ **IISFA** (INFORMATION SYSTEM FORENSICS ASSOCIATION, ITALIAN CHAPTER)
- * Active Member of the **IT Engineer Commission**, Engineers Association of the Latina Province
- * **Digital Forensics Court Trial Witness** on e-crimes and ICT enhanced crimes
- * Consultant for multiple **Law Enforcement agencies** around the world
- * Advisor @ **European Courage Focus Group** – Cyber Terrorism & Cybercrime
- * **ITU Roster of Experts Official Member**
- * **HTCC HIGH TECH CRIME CONSORTIUM Member**
- * Co-Founder at **The Security Brokers**
- * Trainer at **NATO, INTERPOL**
- * **CIFI - Certified Information Forensics Investigator**
- * Certified Trainer for **SPEKTOR & UFED**
- * **ECISO Board of Directors Member**



TERMINOLOGIES

Nel mondo dell'InfoSec abbiamo un *enorme* problema:
la terminologia.

- La quale, a sua volta - e già "sporcata"! - ha **interpretazioni** e **logiche** anche molto diverse, in funzione del **settore** in cui la si utilizza ed applica.

Come se non bastasse, negli **ultimi anni** è scoppiata la **moda** di anteporre il prefisso "cyber" alla maggior parte dei termini.

- **Ciò nonostante**, alcuni (grossi) dubbi persistono...persino per i madrelingua!



Ortografia non omogenea...

„Cybersecurity, Cyber-security, Cyber Security ?”

assenza di definizioni condivise...

Cybercrime é...?

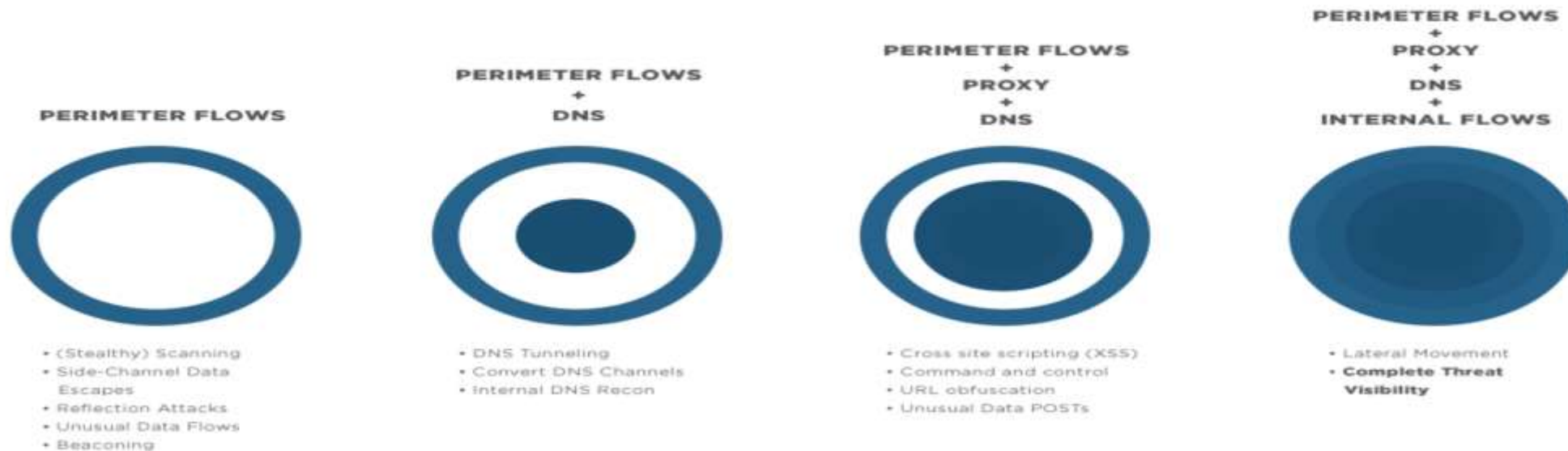
Chi sono gli attori?...

Cyber /crime/war/terrorism ?

Nei paesi non di lingua inglese, i problemi di comprensione aumentano esponenzialmente

“We don’t want to be forensics experts. We want to catch it at the perimeter”

Maj. Gen. Steven Smith, Chief of the US Army Cyber Directorate,
May 5th, 2012



Traditional Crime

CRIME, ORGANIZED

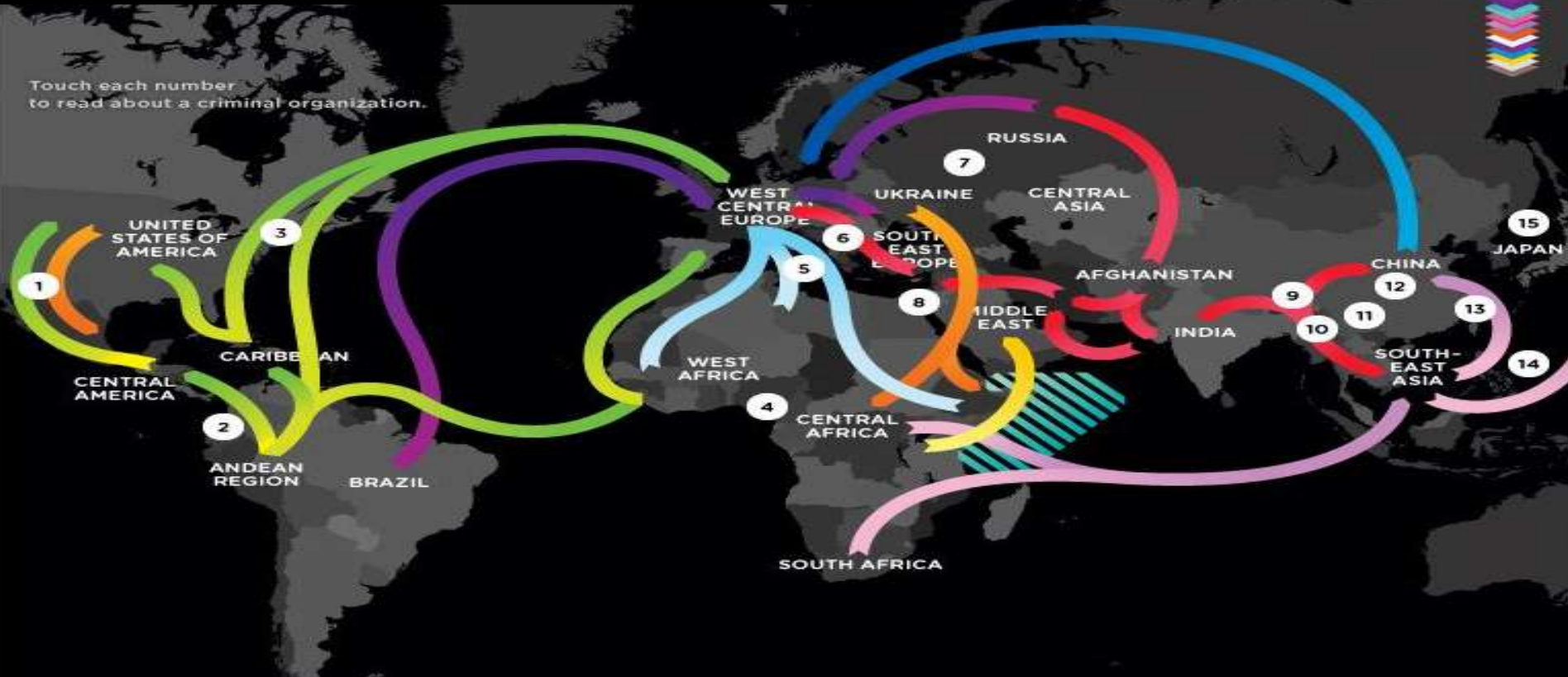
The Mafia, la Cosa Nostra, the Yakuza, Mexican cartels—the underworld is ruled by a complex network of criminal groups. Here's how they fit together.

\$128 billion
Total estimated value of organized criminal activity.

Flow of Transnational Organized Crime

Click the icon to see a breakdown.

Touch each number to read about a criminal organization.



Click each category to see the flow of goods.



- FEMALE TRAFFICKING
- COUNTERFEIT GOODS
- HEROIN
- WILDLIFE
- GOLD
- PIRACY
- FIREARMS
- COCAINE
- MIGRANT SMUGGLING

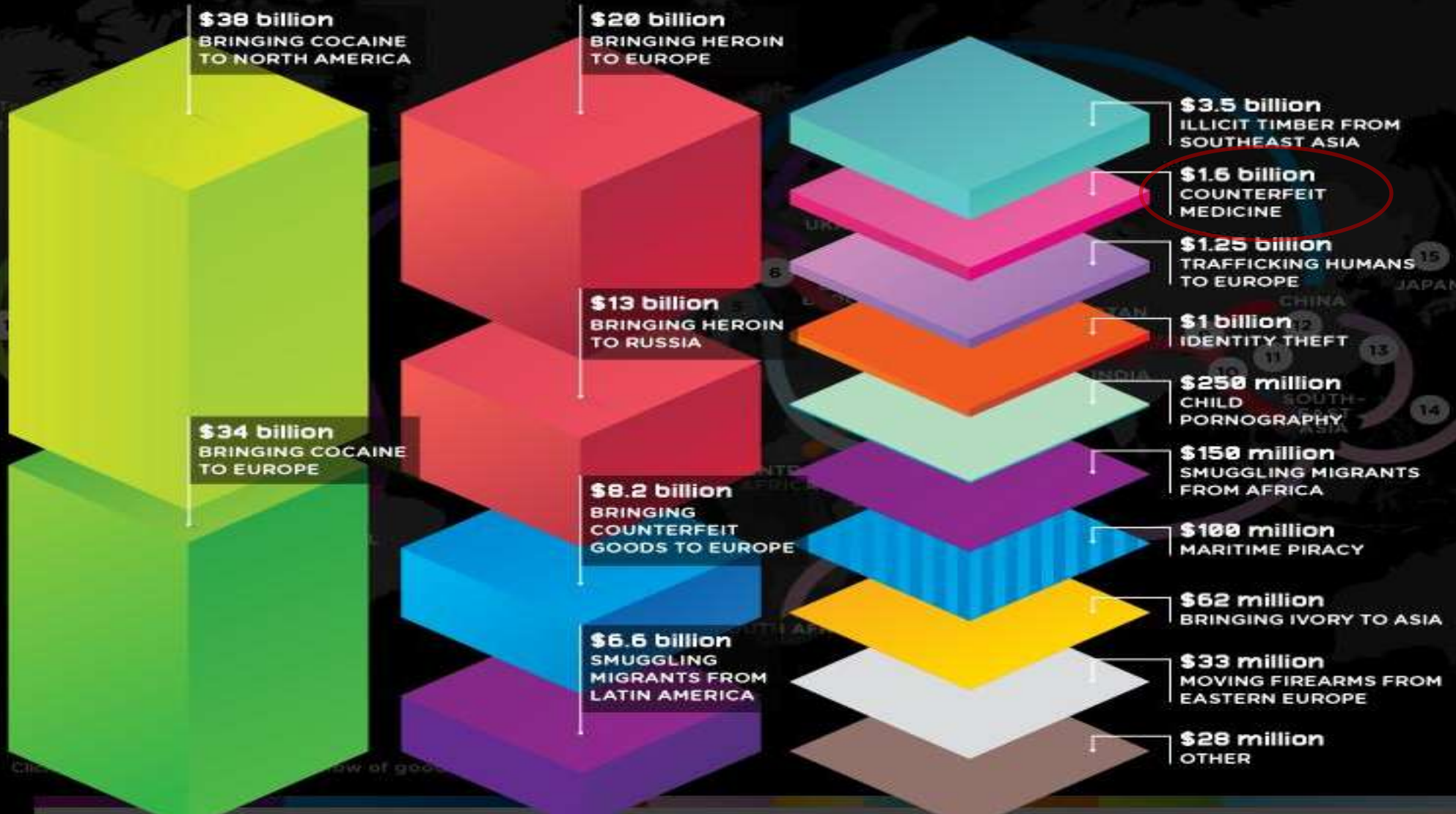


Something has changed!

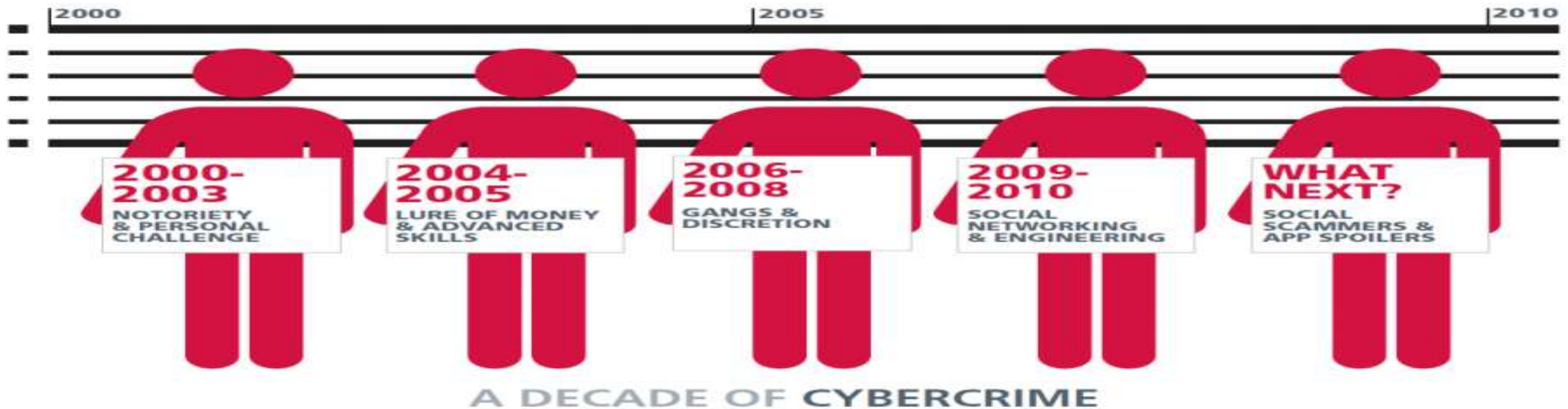
Drugs earn the most and cause the most violence.

Total estimated value of organized criminal activity,

ESTIMATED VALUE OF CRIMINAL ACTIVITIES, BY TYPE

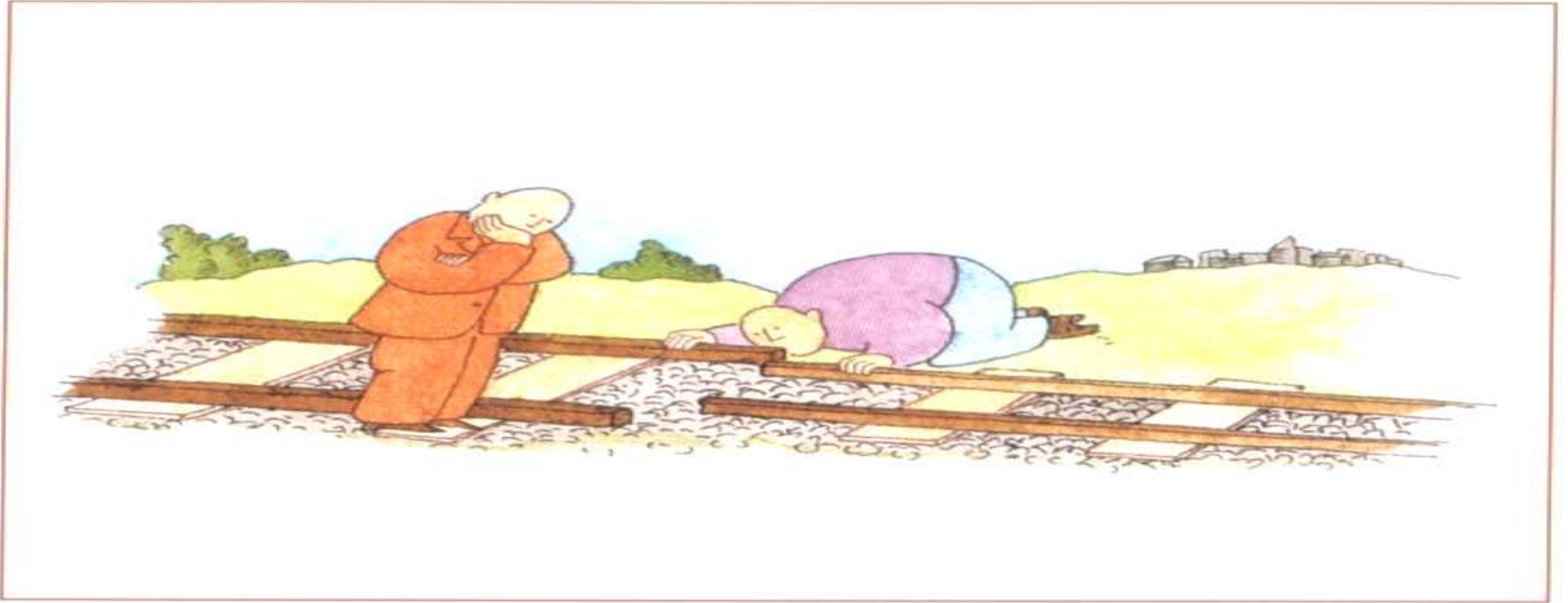



The day money became the focus of malware
is the day the Internet changed
Graham Ingram, AusCERT GM



SOURCE: McAfee

Mindsets and Backgrounds





**ATTACKS ARE A
TECHNICAL PROBLEM,
DEFENSE IS A
POLITICAL PROBLEM**

THOMAS DULLIEN,
"Why we are not building a
defendable Internet" BH ASIA 2017

A man with glasses and an orange shirt is speaking at a podium. The podium has a laptop and a logo for 'black hat ASIA 2017'. The background is a green screen with light effects.

DEAR CISO, WHO ARE YOU MOST SCARED OF?

SAUMIL SHAH
"The Seven Axioms Of Security"
BH ASIA 2017


black hat
ASIA 2017

What's different - nowadays

- * 2 types of (corporate) companies
- * YOUR data are (already) outside of the perimeter
- * GDPR
- * Third-party breaches impact on your infrastructures

CyberSec Expert – skillset

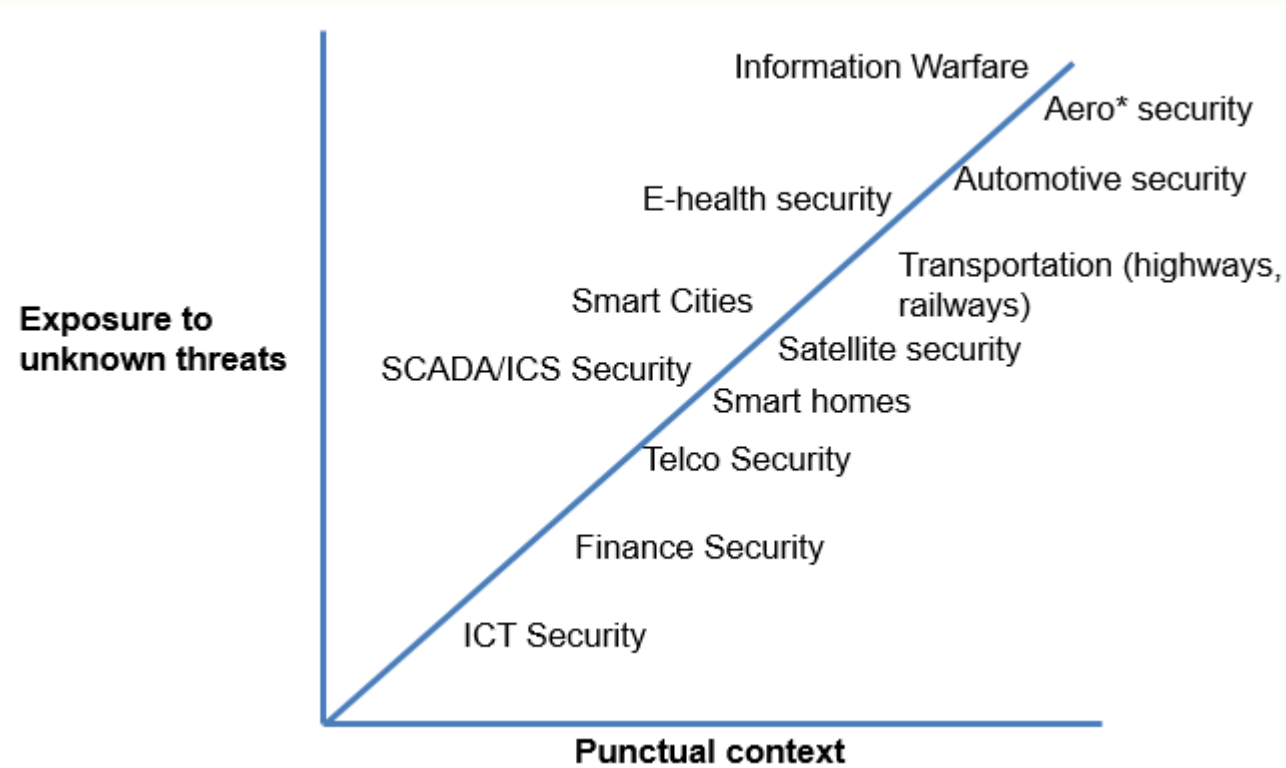


Ing. Selene Giupponi - 2014



Threats

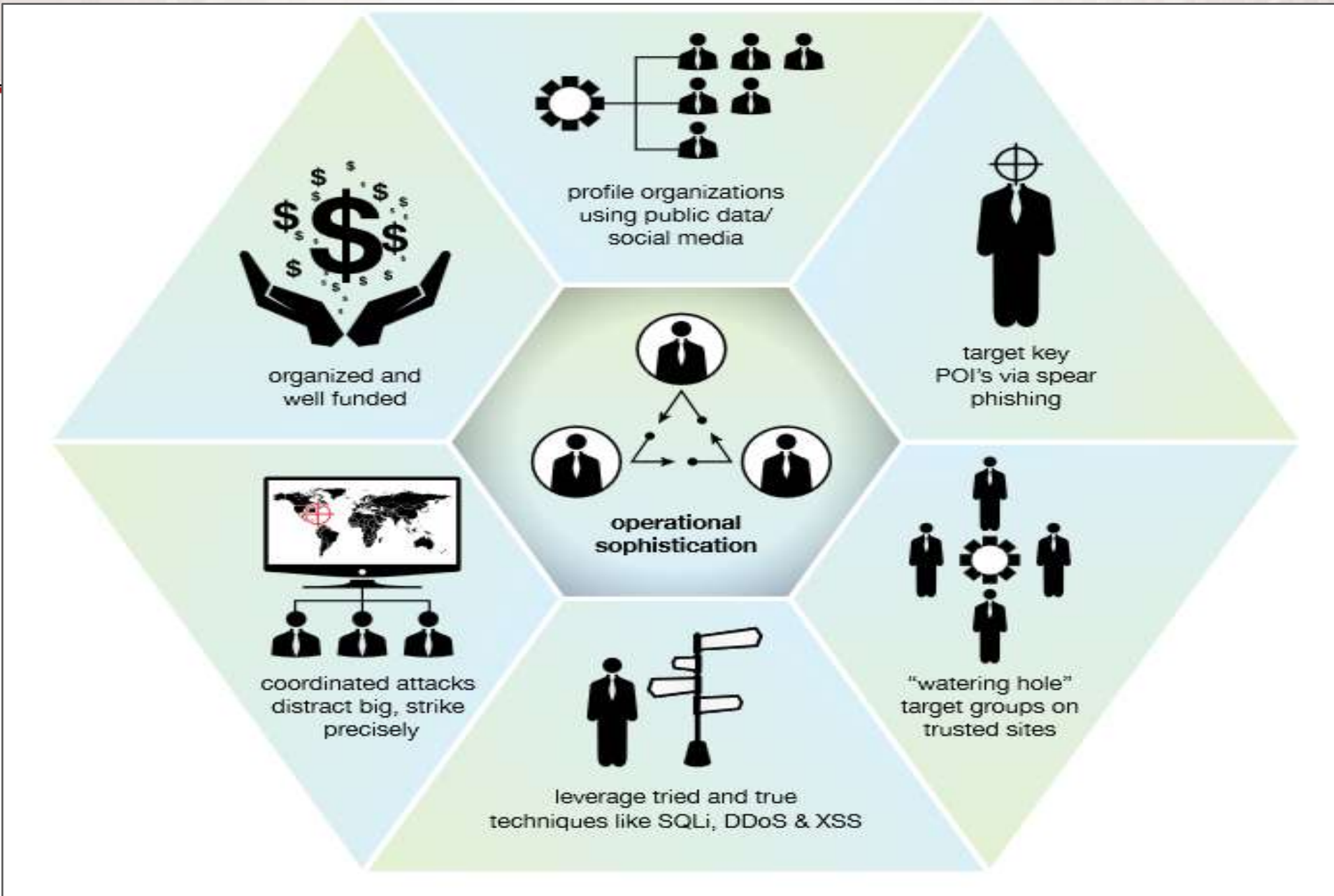
Digital Forensics



Source: SB internal research, 2015-2019

Cyber Threat Intelligence

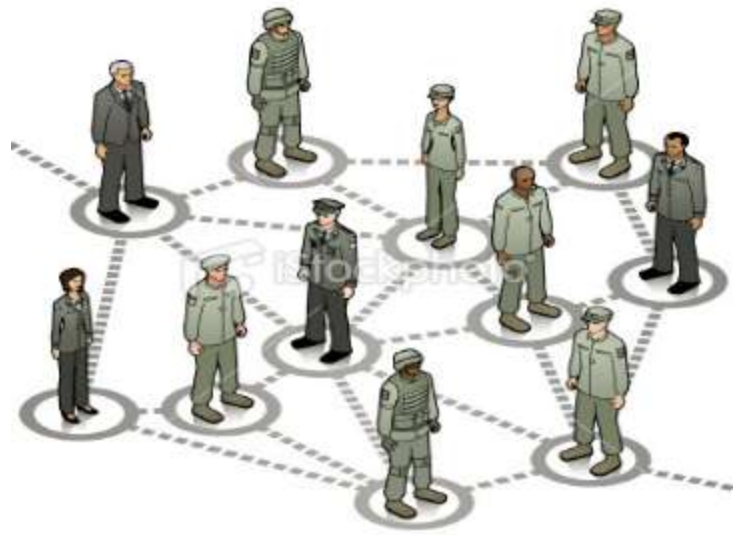




*"I urge you to be more innovative when it comes to emerging threats such as **cyber-crime**, environmental crime and counterfeiting, we must stay one step ahead of the criminals. We must also be more effective in stopping the money flows enabled by corruption and money-laundering"*

Ban Ki-moon, 2010



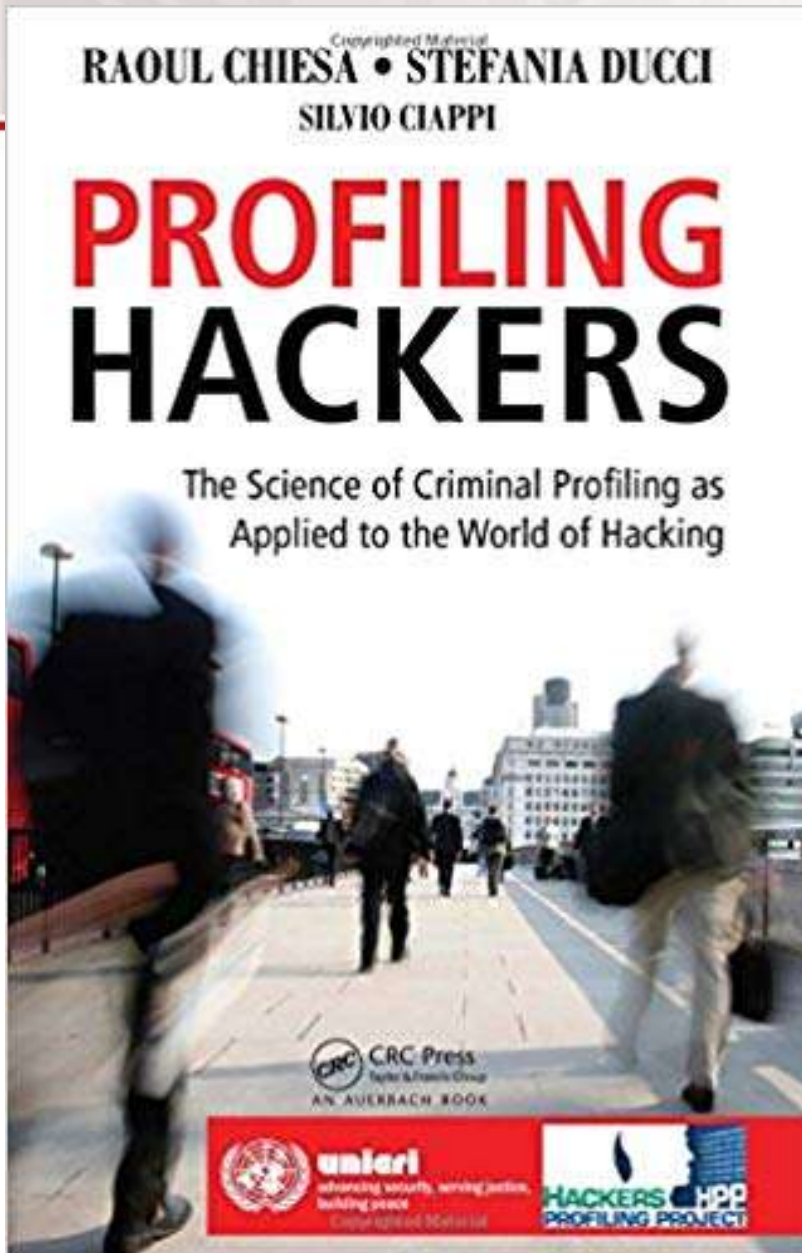


"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is **hackers**

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

Profiling “hackers”



- Applied Research started back in 2004
- Field research started in 2006 (still on-going)
- Law Enforcement Officers and Government Agencies loved our profiling approach
- FBI Academy Library in Quantico (VA)
- Special Agents (cybercrimes) must-read book
- Translated in different languages
- Cutting-edge milestone from the previous “Black-hat / White-hat” approach

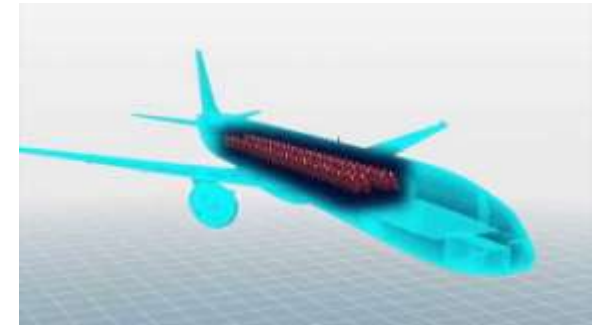
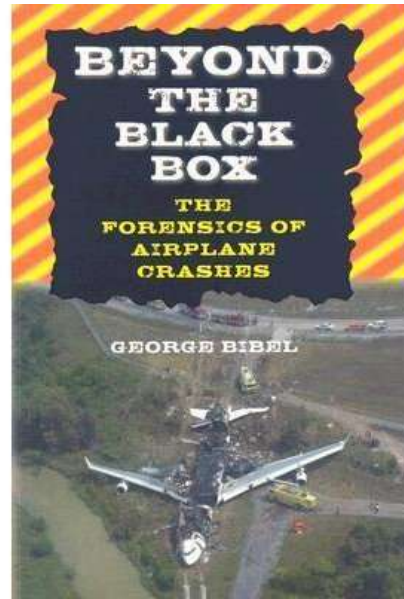
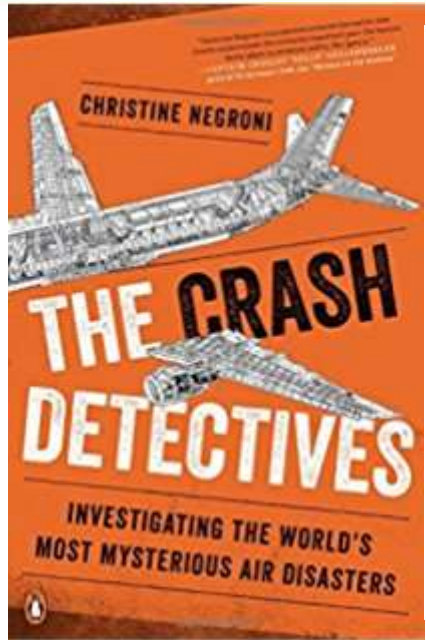




Misha Glenny (Author of “McMafia” and “Dark Market”) while speaking about HPP at TED 2011

http://www.youtube.com/watch?v=6gSwRHScq6M&feature=player_detailpage#t=341s

Our latest field experience



Real data, Actors, Timelines... and correlations

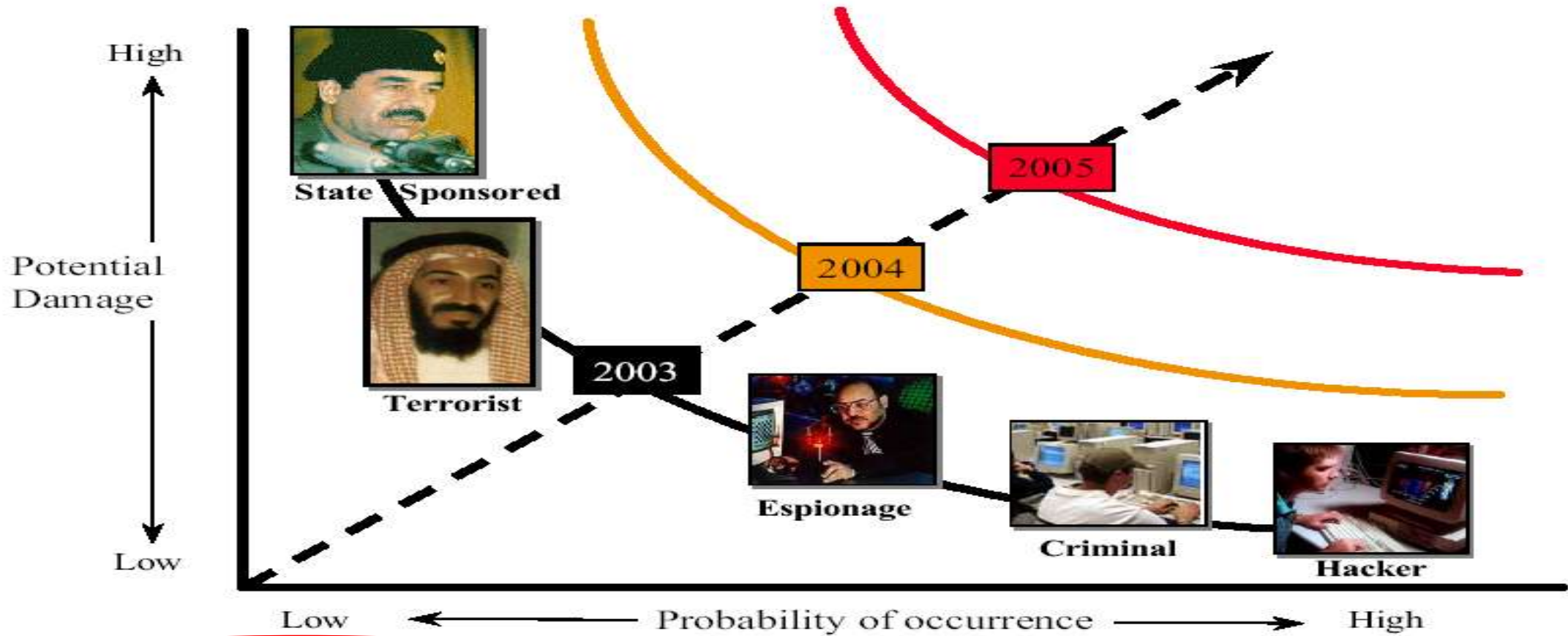
SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

(YOU SHOULD HAVE BEEN AT THE CONFERENCE!)

Today's Oil

- * Information it's the Oil of 21st Century
- * Information = Power
- * Information = Data
- * Data = Bit & Bytes (Files: .ppt, .txt, .doc, .passwd...)
- * Data = Money, Reputation, Impacts, Regulations, Fines

The Threat is Increasing



Source: 1997 DSB Summer Study

- Hackers / Hacktivists Groups
 - .ANONYMOUS ACTIONS
 - .Cybercrime / Criminal Gangs
 - 4chan
 - 8chan
 - A99
 - Activists - Disrupt Dirty Power Action
 - Activists - background information and reports
 - Afghan Cyber Army
 - Ag3nt47
 - Ajan Turkish Hacker
 - Ajax Security Team / Operation Saffron (Iranian hacker group)
 - Al-Qaeda Electronic Army
 - AnonGhost
 - Antisec / Anti-Sec Movement
 - BlackKatSec
 - China Blue Army
 - Conspiracy Cells of Fire - CCF
 - CyberBerkut /cyber berkut - Ukrainian hacktivistsUkrainian
 - European Cyber Army / AntiSec / ECA_Legion
 - Evil - Australia
 - Free Syrian Hacker Group / Dr.SHA6H
 - Ghost Shell / Ghostshell/TeamGhostShell
 - Global Islamic Media Front
 - Goatse Security
 - Hacker groups / Hacktivists - Various
 - Hidden Lynx
 - HighTech Brazil HackTeam / hack team
 - Iranian Cyber Army
 - Islamic Cyber Resistance (ICR)
 - Islamic State Hacking Division (ISHD)
 - IsraeliElite / OpIslam
 - Kdms Team aka Anonymous Palestina

New Fields of Application and Research



World Economic Forum Report(s)

Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Failure of climate-change mitigation and adaptation
- 3 Natural disasters
- 4 Data fraud or theft
- 5 Cyber-attacks
- 6 Man-made environmental disasters
- 7 Large-scale involuntary migration
- 8 Biodiversity loss and ecosystem collapse
- 9 Water crises
- 10 Asset bubbles in a major economy

Top 10 risks in terms of Impact

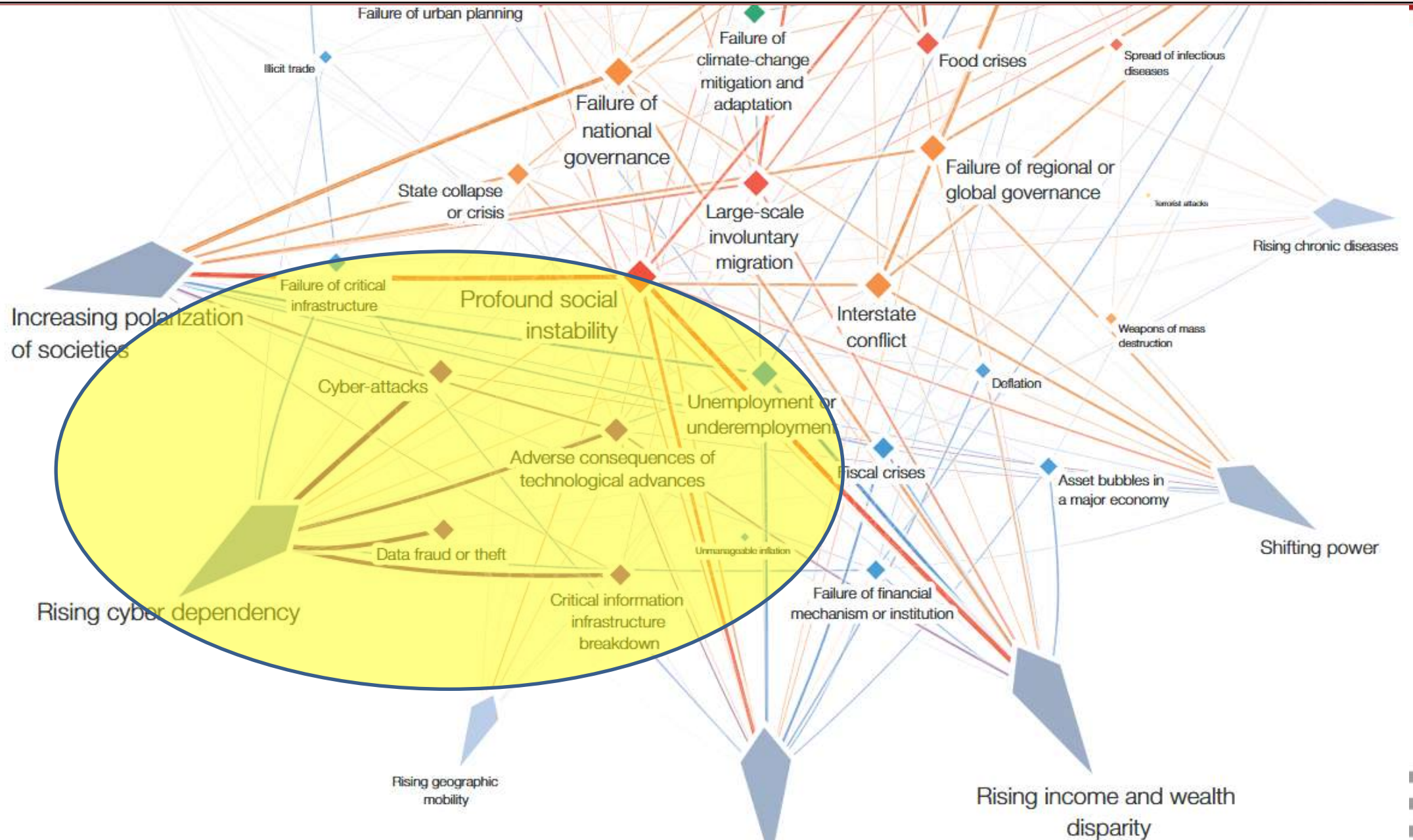
- 1 Weapons of mass destruction
- 2 Failure of climate-change mitigation and adaptation
- 3 Extreme weather events
- 4 Water crises
- 5 Natural disasters
- 6 Biodiversity loss and ecosystem collapse
- 7 Cyber-attacks
- 8 Critical information infrastructure breakdown
- 9 Man-made environmental disasters
- 10 Spread of infectious diseases



Categories

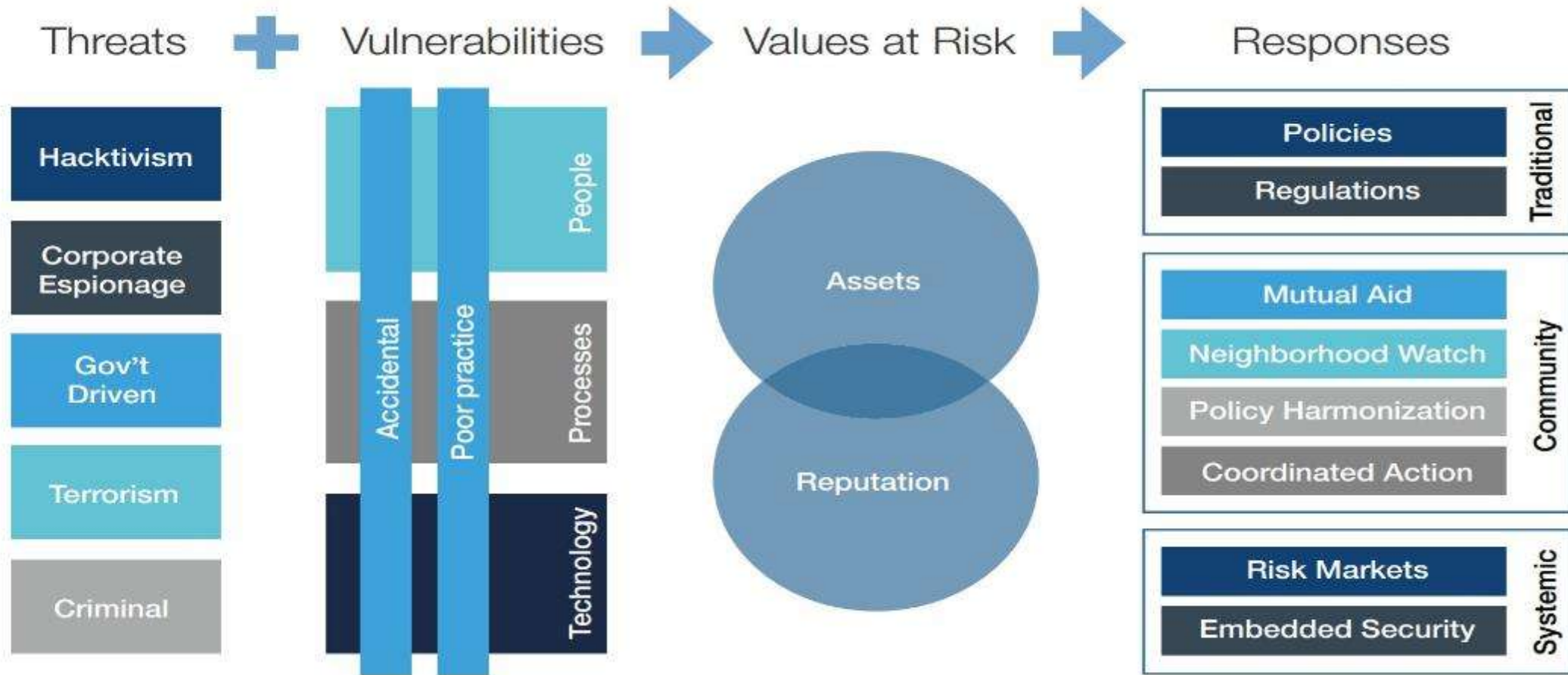
- Economic
- Environmental
- Geopolitical
- Societal
- Technological

World Economic Forum Report(s)



World Economic Forum Report(s)

Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum

Conclusions

- * **Every new approach typically leads to new methodologies, because we all need to standardize what's brand new.**
- * **In our case, both DF and CTI (rather than Audit VS Proactive approaches, etc..) have their own standards, languages, and correlation flows.**
- * **What's still missing is field experiences, in order to enhance a new way to (dramatically) kick the ass of the bad guys, and optimize the way we can support the Internet Security Industry and the Law Enforcement against Cybercrime, and those crimes supported or backed-by ICT.**

Just married

- * There's a **long way to go...**
- * This love story **just began!**
- * Different educational backgrounds will need to **understand each other's** much better, learn the concept of **mutual trust**, experience **incidents**, and **learn from the real-life**, in the **good** and the **bad** times.



Question Time

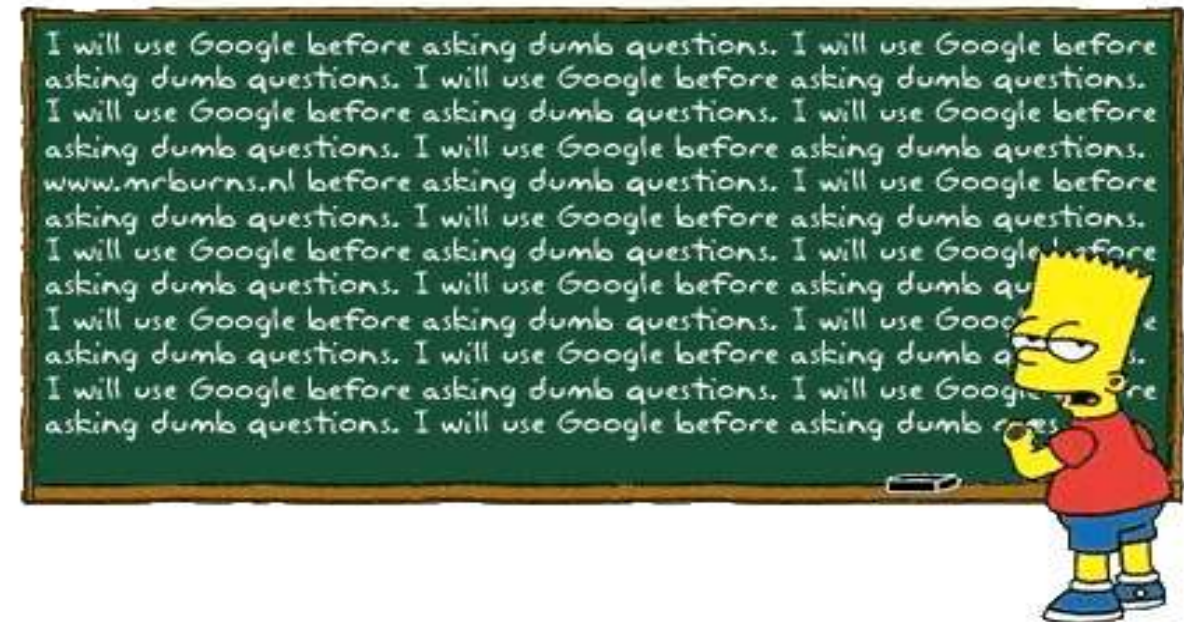
Raoul “Nobody” Chiesa

[rc \[at\] security-brokers \[dot\]com](mailto:rc[at]security-brokers[dot]com)

Eng. Selene Giupponi

[selene.giupponi \[at\] resecurity.com](mailto:selene.giupponi[at]resecurity.com)

Thanks for your attention!



SecurityBrokers

GLOBAL CYBER DEFENSE & SECURITY SERVICES



Security Brokers scpa

Via Appia Nuova, 113 - 00183 Rome Italy

Email: info@security-brokers.com - Website: <http://www.security-brokers.com>