Strategic Decision Making Course: a Exercise on Cyber Crisis
National Defence Institute, 13May14

10th UIC World Security Congress Lisbon 2014

Security Events Impacting the Rail System
(at the Operations, Economic an reputation levels)

Lisboa, 28 November14

Cyber Defence Response

– A Strategic Challenge –

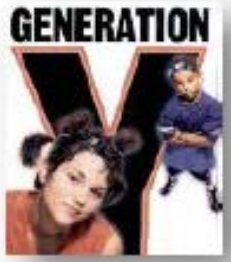
Lt Col Paulo Viegas Nunes
nunes.pfv@mail.exercito.pt

Agenda

- Cyberspace Strategic Impact
- Information Warfare: a new Operational Paradigm
- Social Risk Management
- Cyber Security and Cyber Defense
- National Cyber Security Strategic Concept
- Conclusions

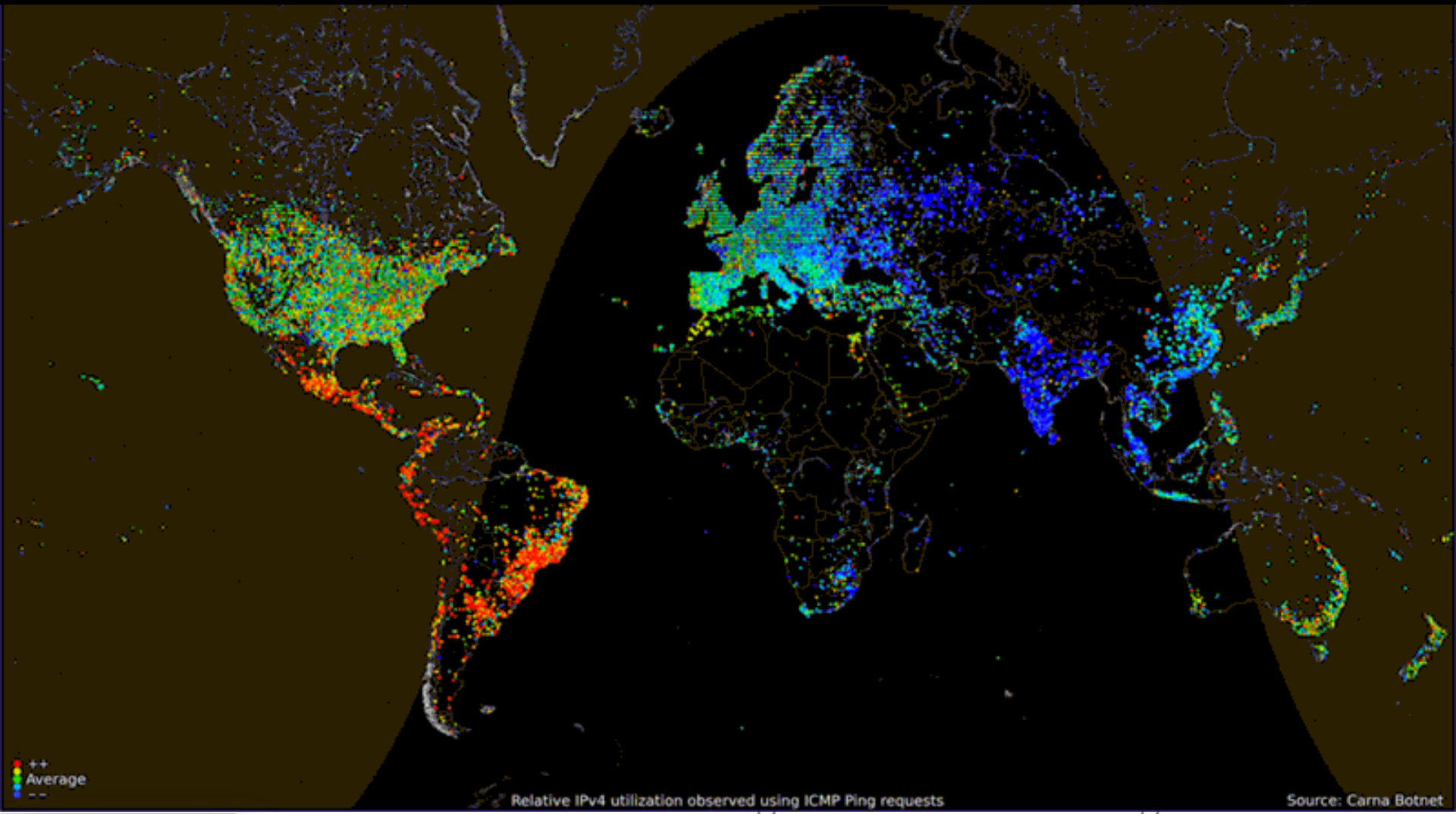
Technical (Re) Evolution – Profiles and Generations

1946-1964 | 1965-1980 | 1981-2000 | …2017 | ?



Adaptado de:

Cyberspace - "A New Global Common..."

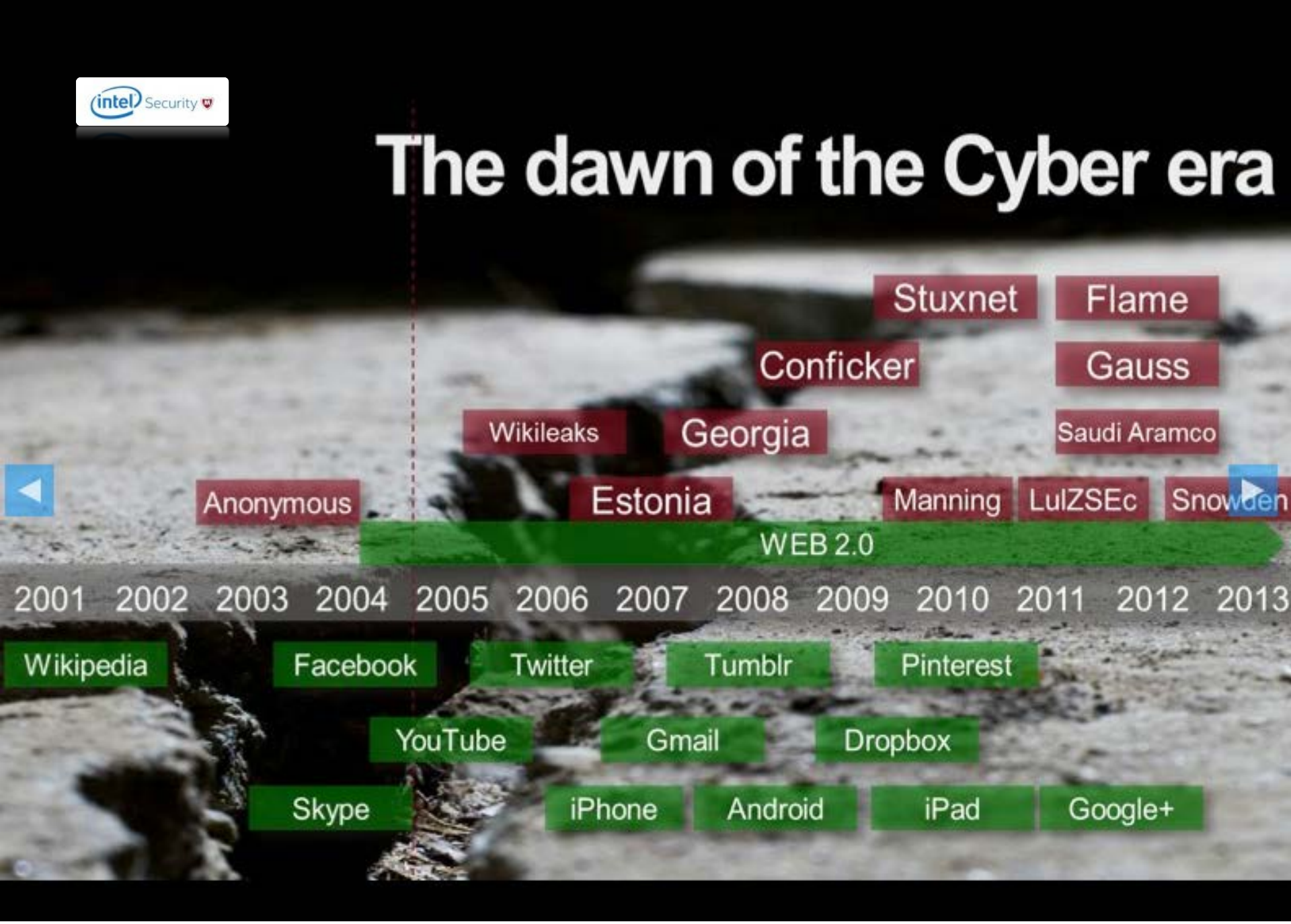


Money

Multi-User

Multi-Proprietary

The dawn of the Cyber era



“Do the Ends justify the Means” ?

The “Obama Effect” - Schedule of Events

2007 – “Defensive mindset in cyberspace”

2009 – Stuxnet Deployed

2010 – US CYBERCOM Operational

2011 – US Cyber Strategy

2012 – US Air Force: **Cyber Operations at local Commander’s discretion**

2013 – US Preemptive Cyber Strategy

Source:Ralph Langner, Lagner Communications GmbH; 28Sep12

Operational Costs vs Reach

$90B Nuclear Sub Fleet

$40B Stealth Fighter Fleet

$10B Euro Fighter Fleet, Leopard II Group

$1B Cyber weapons Program, MIL Targets

$100M Cyber weapons Program, CI Targets

$5M Singular cyber attack against National Critical Infrastructures

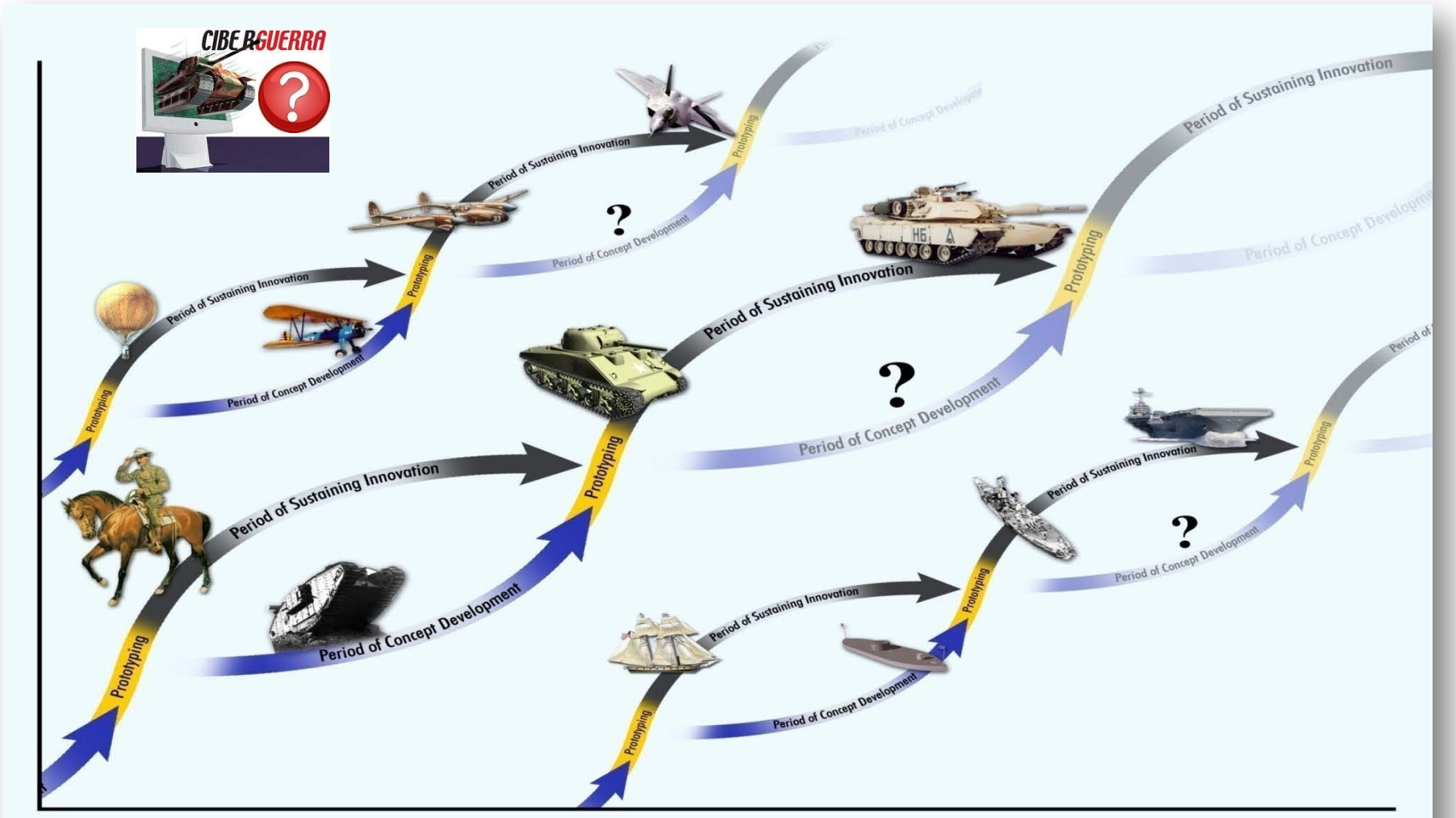
non-state actors threshold

Source:Ralph Langner, Lagner Communications GmbH; 28Sep12

Information Warfare: A Paradigm Shift

To wage non kinetic conflicts

Military Innovation
Concept Development and Experimentation



Source: Dennis Popiela; Delivering Innovation ; Joint Concept Development and Experimentation MITRE Corp.

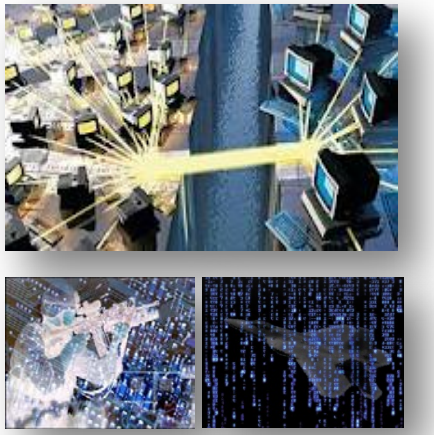
Cyberspace: 4+1 Dilemma …

+

4+1?

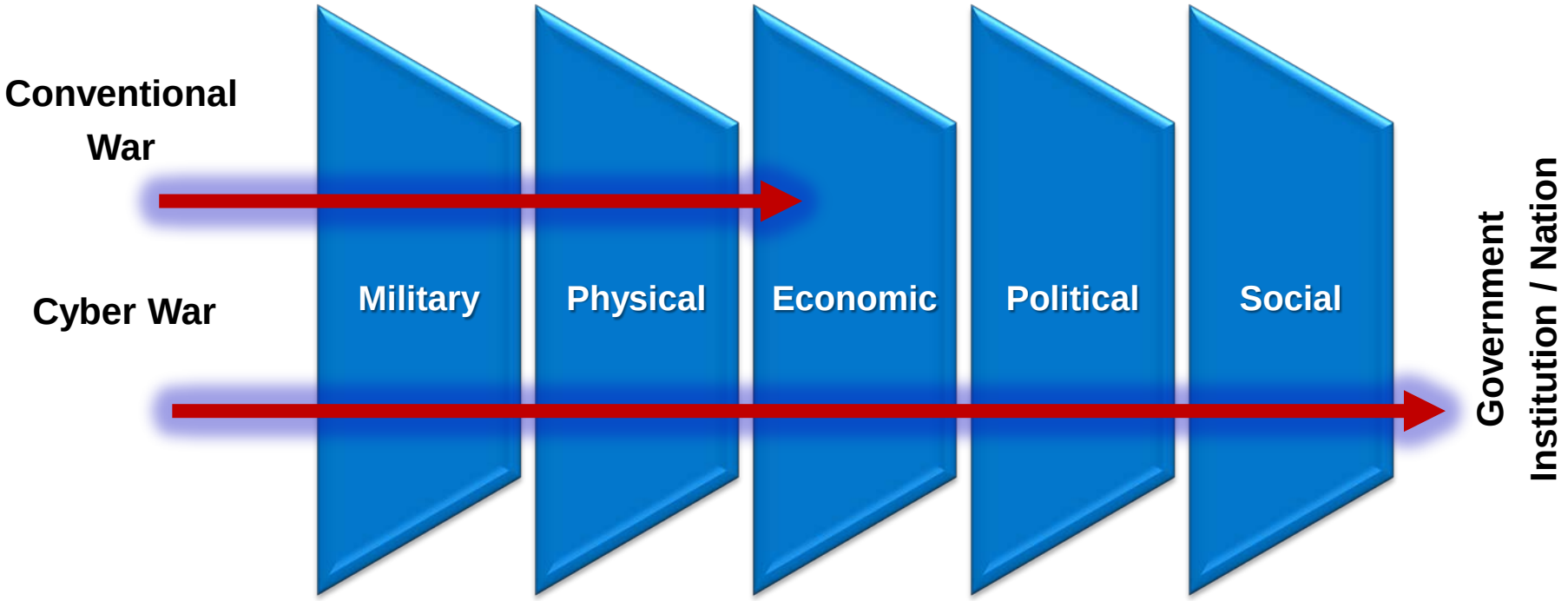
or

SUBDOMAIN !!



or the 2!!

Cyber War Impact

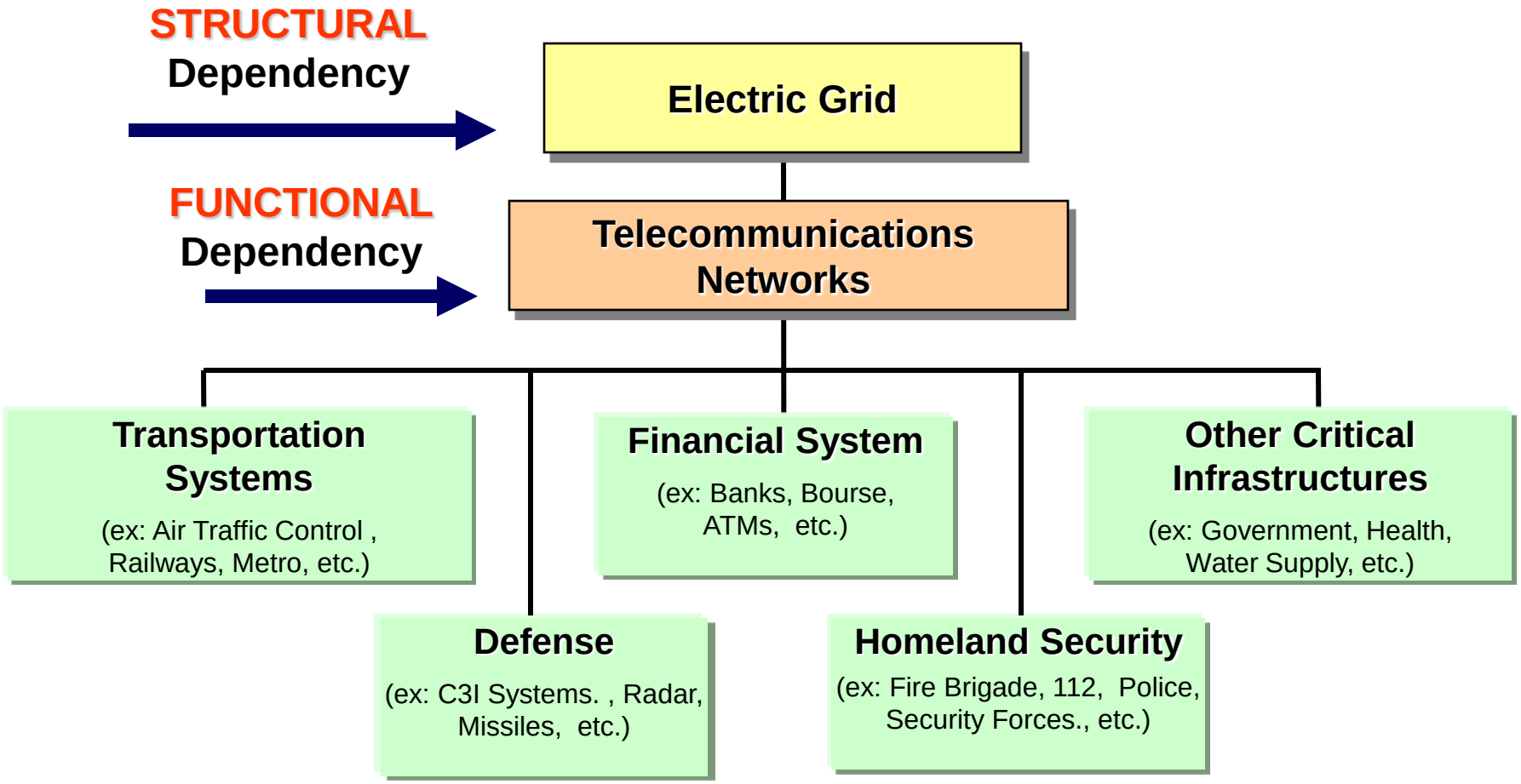


"Os verdadeiros alvos são a mente dos Decisores e Comandantes, não os seus Exércitos ou as infraestruturas impenetráveis que os protegem"

(autor desconhecido)

Social Risk Management – Cyber Impact

National Critical Infrastructures :
Interdependency Model



Source: Adapted Gen Pinto Ramalho (2003); Eng. Sousa Cardoso (2003).

Global Risks (2007-2014)

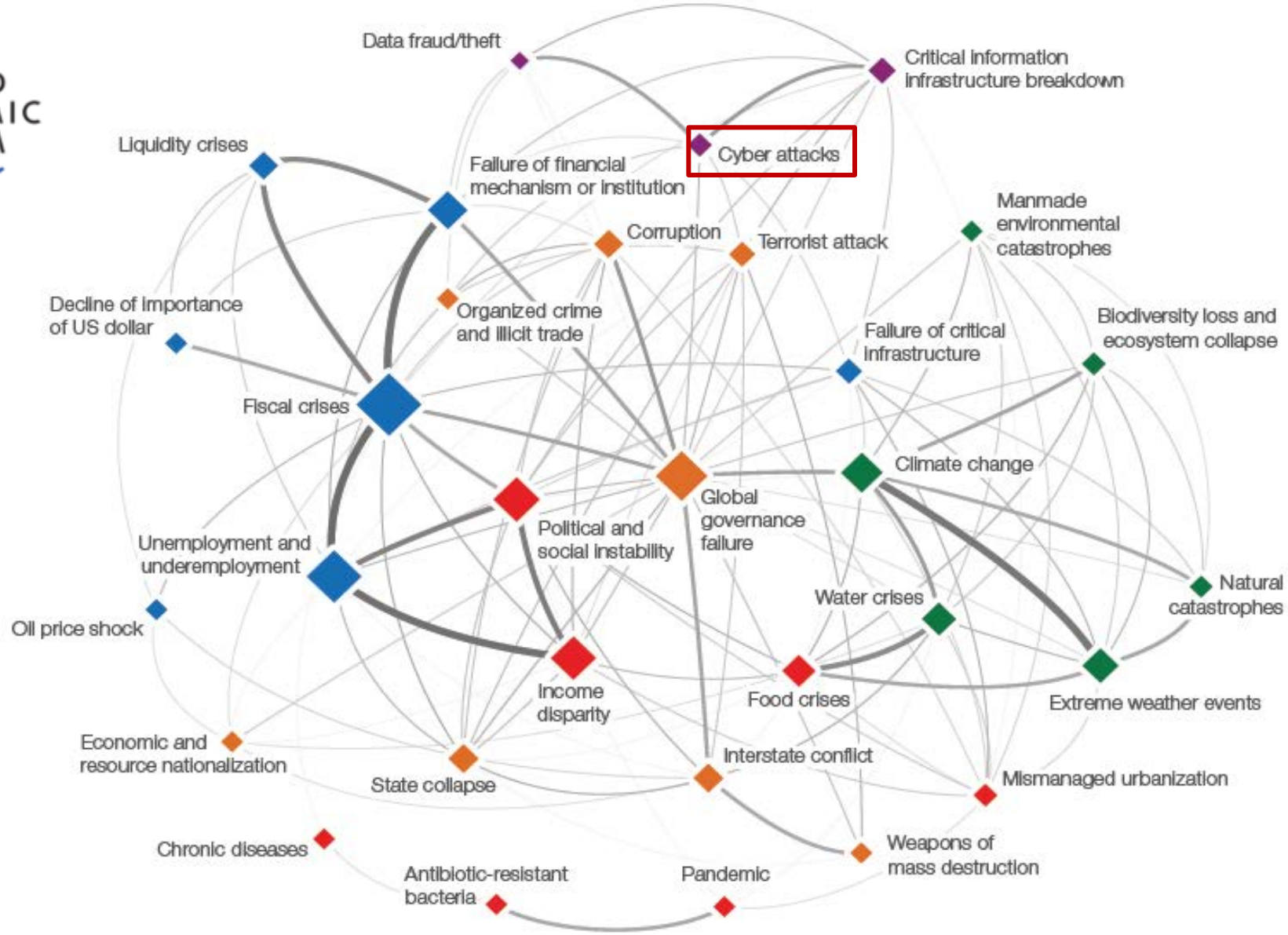
Top 5 Global Risks in Terms of Likelihood

WORLD ECONOMIC FORUM

	2007	2008	2009	2010	2011	2012	2013	2014
1st	Breakdown of critical information infrastructure	Asset price collapse	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity
2nd	Chronic disease in developed countries	Middle East instability	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events
3rd	Oil price shock	Failed and failing states	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment
4th	China economic hard landing	Oil and gas price spike	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber attacks	Water supply crises	Climate change
5th	Asset price collapse	Chronic disease, developed world	Retrenchment from globalization (emerging)	Global governance gaps	Climate change	Water supply crises	Mismanagement of population ageing	Cyber attacks

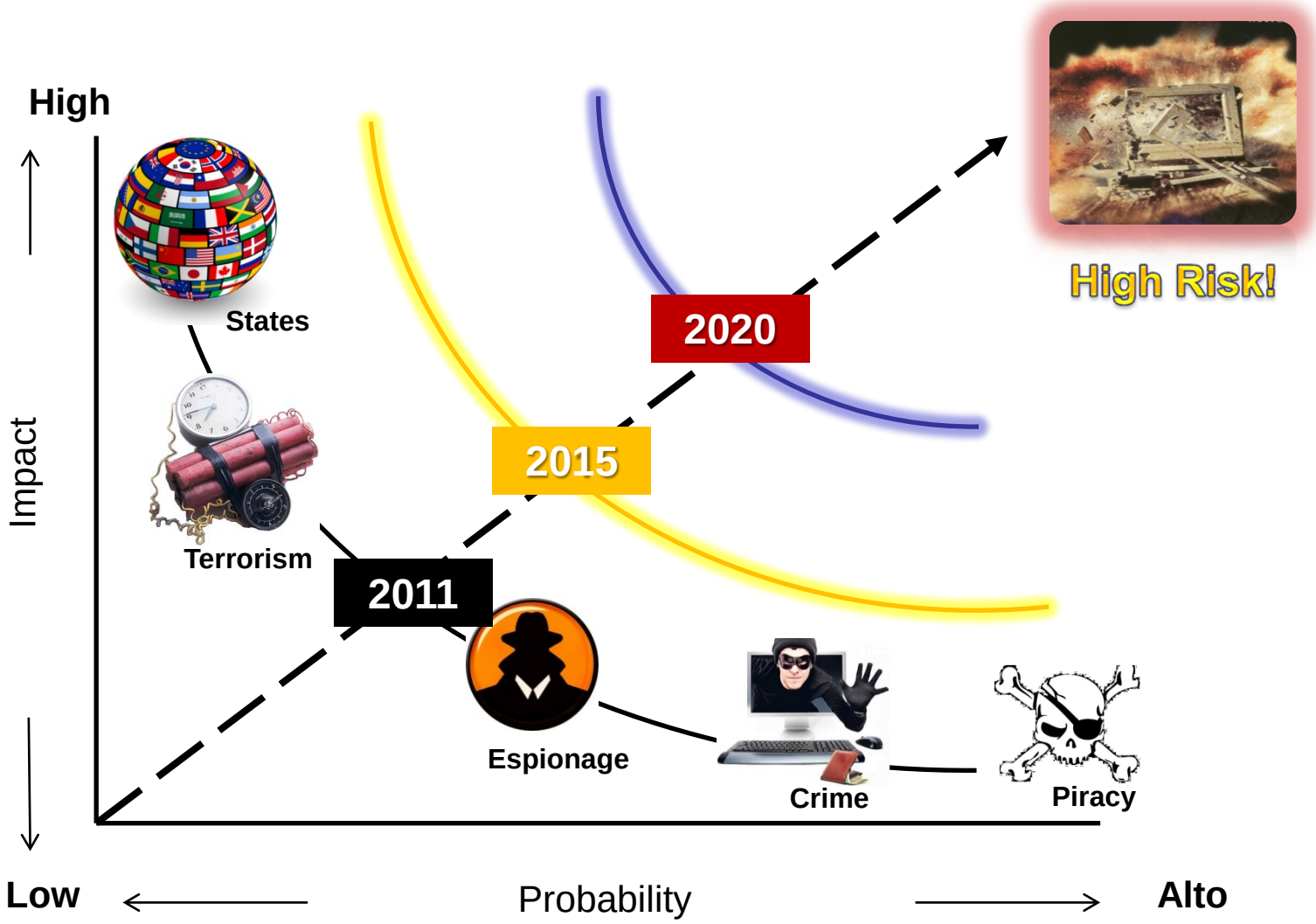
Fonte: WEF, Global Risks Report 2014

Global Risks 2014 – Interconnections Map



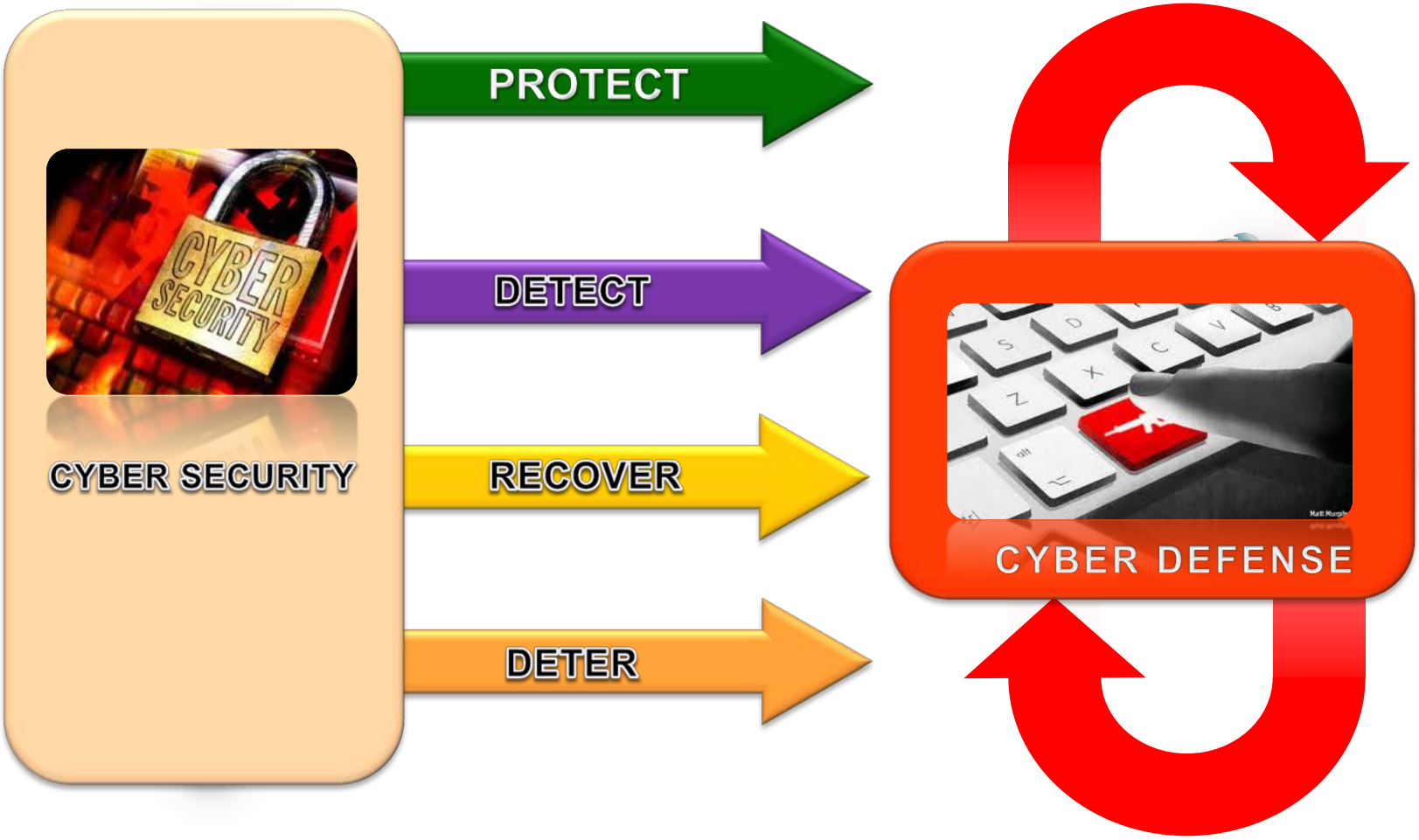
Source: WEF, Global Risks Report 2014

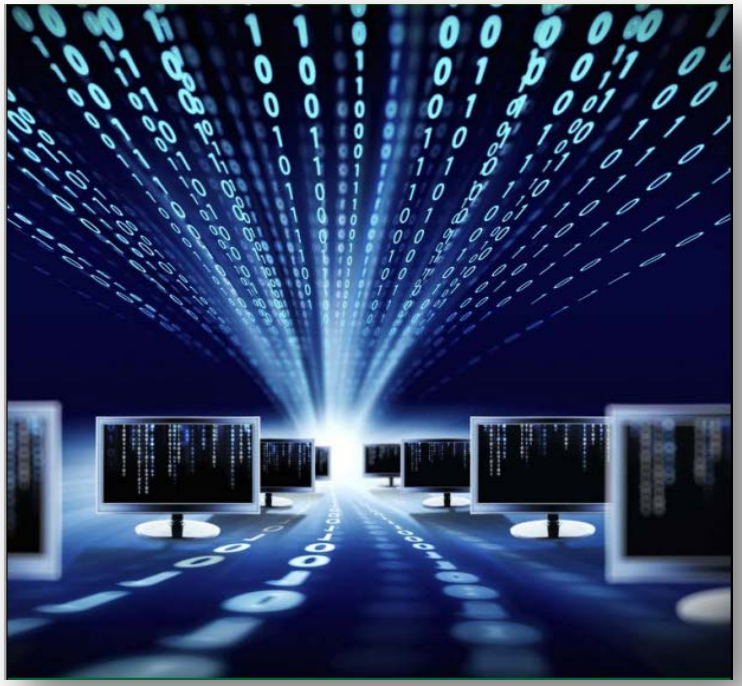
Threat Spectrum – Future



« SYSTEM FAILURE »

Social Risk : What can we do about it?

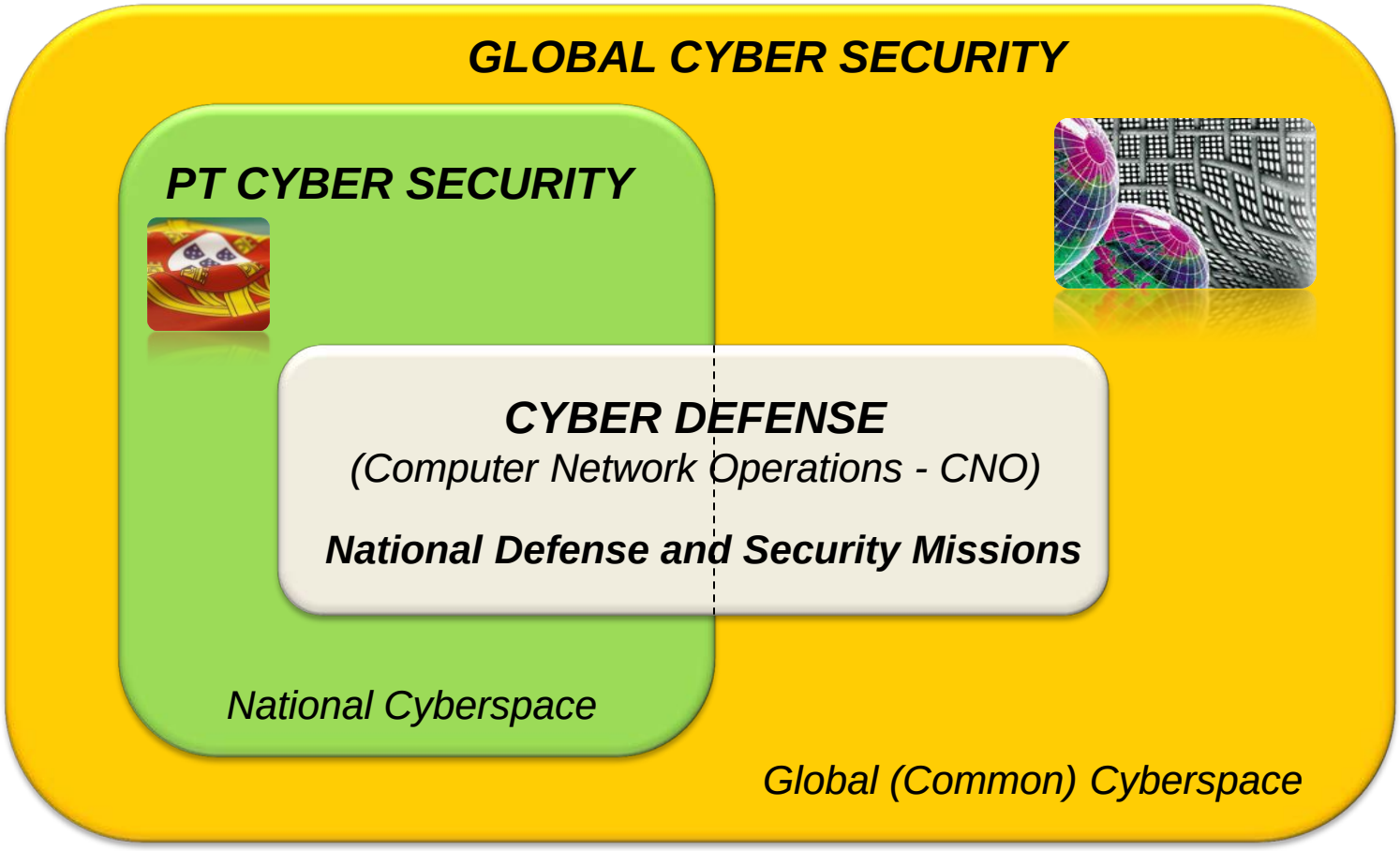




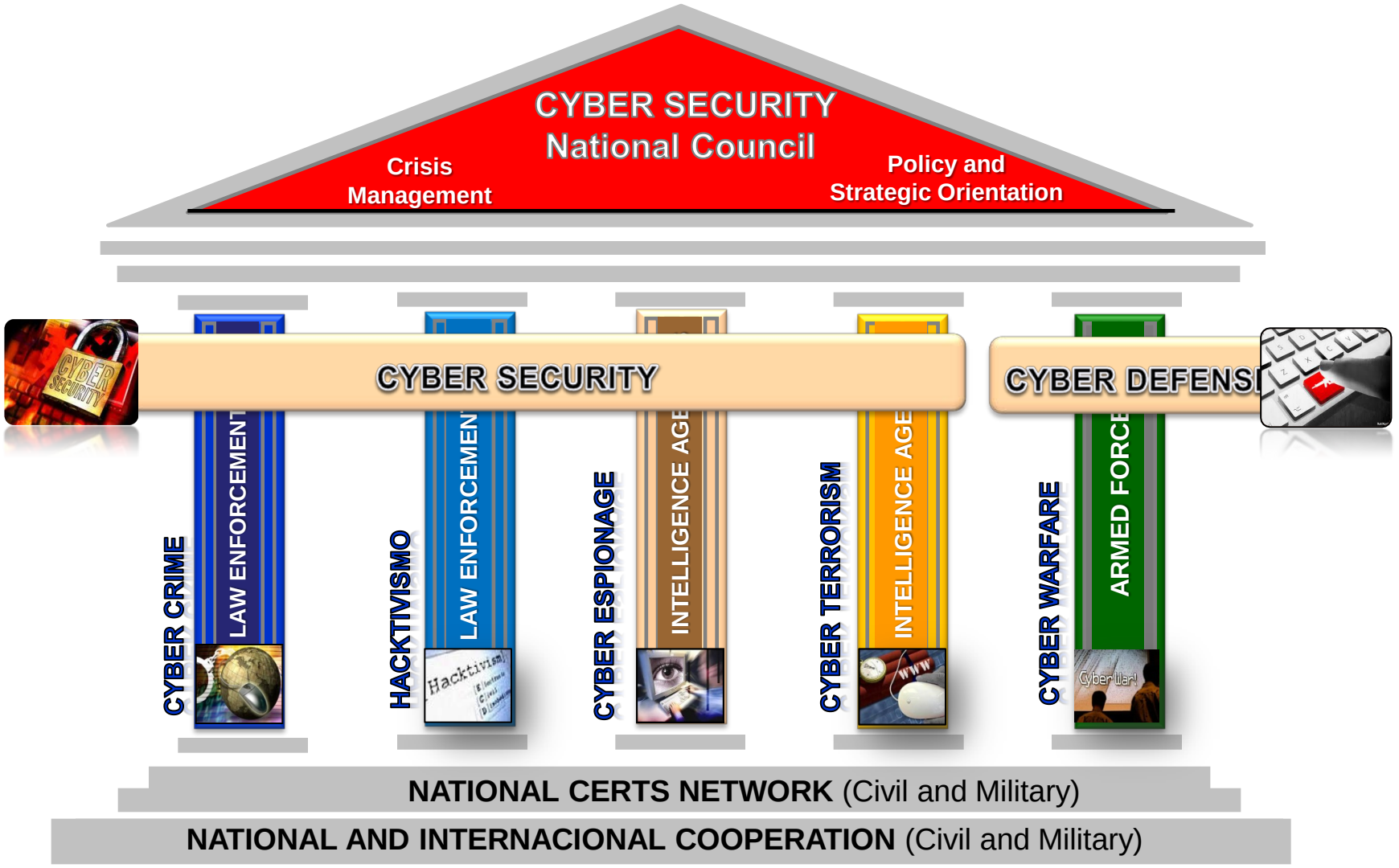
CYBER SECURITY and CYBER DEFENSE:

Protection and Defense of NII
Relevant Questions

Cyber Security vs Cyber Defense



Cyber Security and Cyber Defense:
"One house, several pillars"



"In our interconnected world, we will either succeed collectively or fail individually."

Anders Fogh Rasmussen, NATO Secretary General

National Cyber Security Strategy

(from vision to action)

Strategic Approach: From Vision to Action

National Interests

Principles and Strategic Goals

Aim

(Level of Ambition)

Objectives

Measures

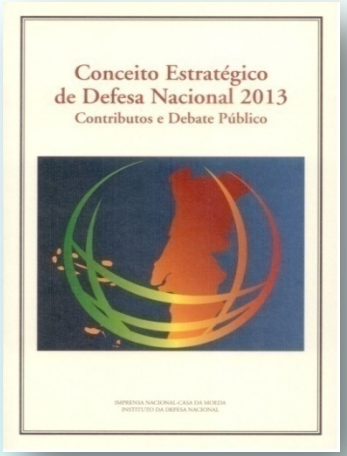
Promote and Reinforce National Strategic Potential

National Cyber Security Strategy:
Aim, Objectives and Measures

Aim	Objectives	Measures
Information Assurance ▪ Secure and efficient use of Cyberspace; ▪ Protection and Defense of National Critical Information Infrastructure ▪ Information Security and Cyber Defense	**Secure use of Cyberspace** (*Generate and Protect Value*)	▪ Analyse Information environment and anticipate attacks; • Detect and block attacks, alert and support potential victims; • Enhance R&D to promote National technological independence; • Adapt Legal framework and fight Cybercrime; • Develop international cooperation initiatives • Communicate, raise awareness and inform citizens
	Reinforce Cyber Security of National Critical Infraestruturas (*Reduce Social Risk*)	• Reinforce Governmental Networks ICT Security; • Reinforce Government and Critical Infrastructures IS Security (Resilience and Survival);
	Defend National Interests and Freedom of Action in Cyberspace (*Reaffirm National Identity and Defend National Sovereignty*)	• "Knowledge and Information Society" initiatives; • Protect and Defend National E-Gov; • National Cyber Security and Cyber Defense Structures; • National Synergies and International Cooperation

Cyber Defence Political Guidance : From Vision to Action

The Strategic Vector
"Information and Cyberspace Security"
(Objectives and Lines of Action)



National Defence Strategic Concept 2013
(RCM Nº 19/2013, 05Abr13)

Strategic Vision

"Defence 2020" Reform
Despacho MDN,
Nº 7527 –A/2013
(31Mai13)

GOVERNO DE PORTUGAL | MINISTÉRIO DA DEFESA NACIONAL

National Cyber Defence Capability Implementation Plan

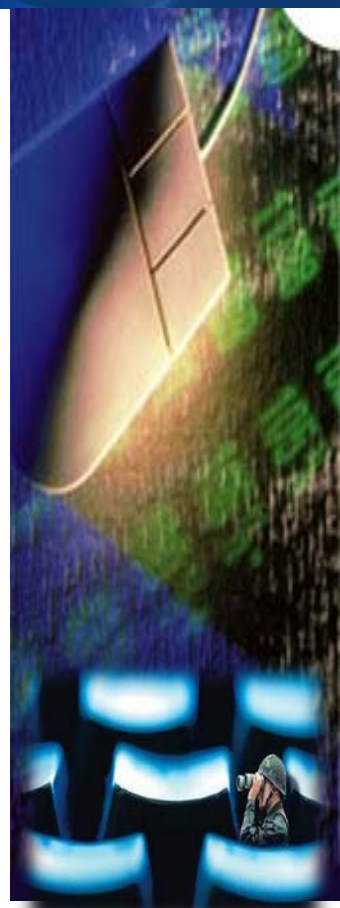
Despacho MDN,
Nº 13692/2013,
(11Out13)

Cyber Defence Political Guidance

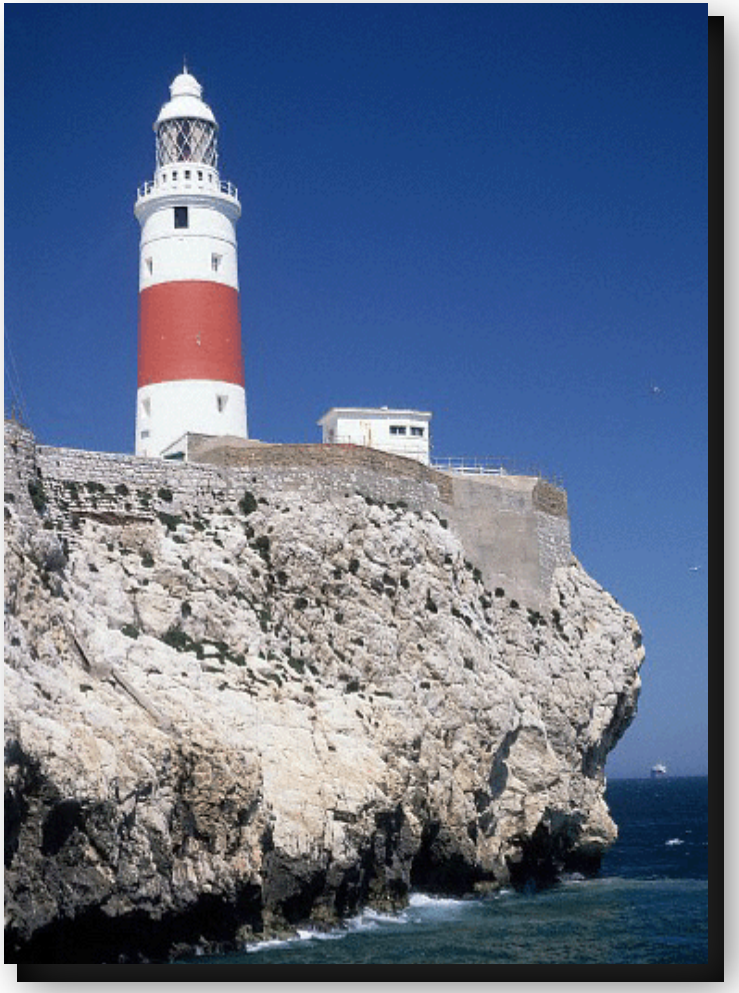
Initiating Directive
(Principles, Objectives and Guidelines)

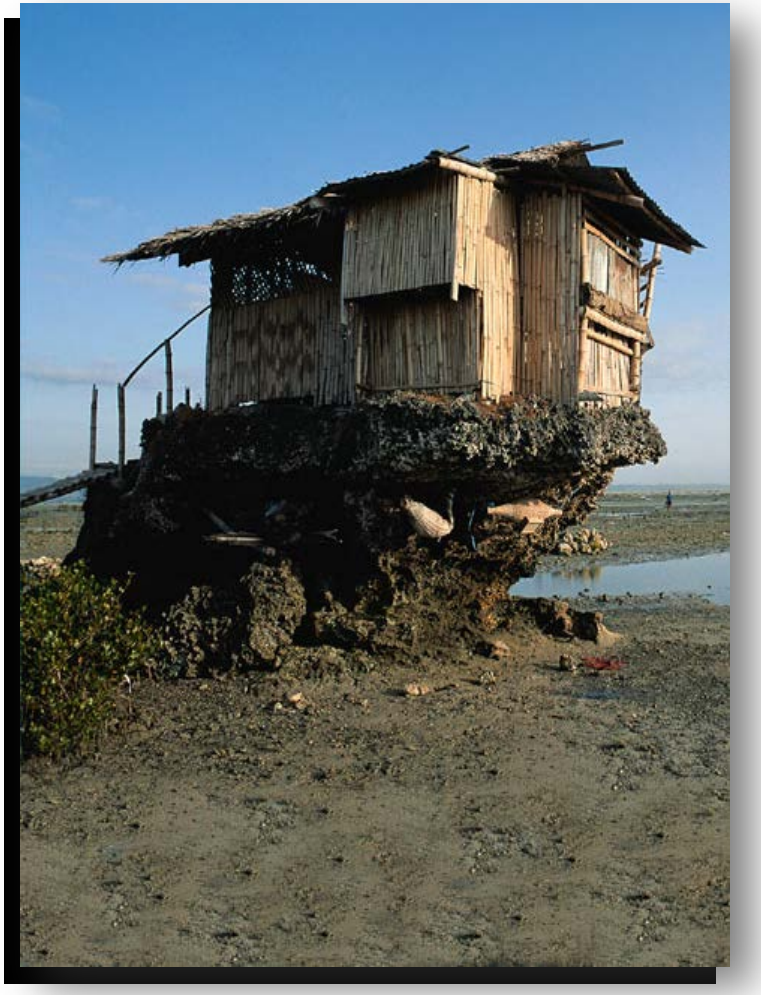
Conclusions

- **Cyberspace is not limited:** individual/collective**;** public/private; civil / military or national / international (Networked Society);
- Cyberspace is **the 5th Operational Domain of modern warfare**, influencing all the physical domains (land, sea, air and space)
- Cyberspace is a **priority strategic domain** where national values and interests must be defended (**non negotiable**);
- Building a **digital future** requires a **National Cyber Security Strategy**
- **Legal Framework**, **doctrine, governance/organization** and **means** to implement a National Cyber Security Strategy
- Clarify **Cyber Security vs. Cyber Defense** concepts
- **National Cyber Security and Cyber Defense** are mandatory for Information Age Societies – NATO and EU Directives



How should the Future be build ?





Questions?
Thank You!

Strategic Decision Making Course 2: Exercise on Cyber Crisis
National Defence Institute, 13May14

10th UIC World Security Congress Lisbon 2014

Security Events Impacting the Rail System
(at the Operations, Economic an reputation levels)

Lisboa, 28 November14

Cyber Defence Response

– A Strategic Challenge –

Lt Col Paulo Viegas Nunes
nunes.pfv@mail.exercito.pt