Novos desafios à segurança e resiliência dos sistemas de comunicações

Paulo Esteves Veríssimo
University of Luxembourg, SnT
CritiX Lab (Critical and Extreme Security and Dependability)

paulo.verissimo@uni.lu
http://wwwen.uni.lu/snt/people/paulo_verissimo

Stage setting

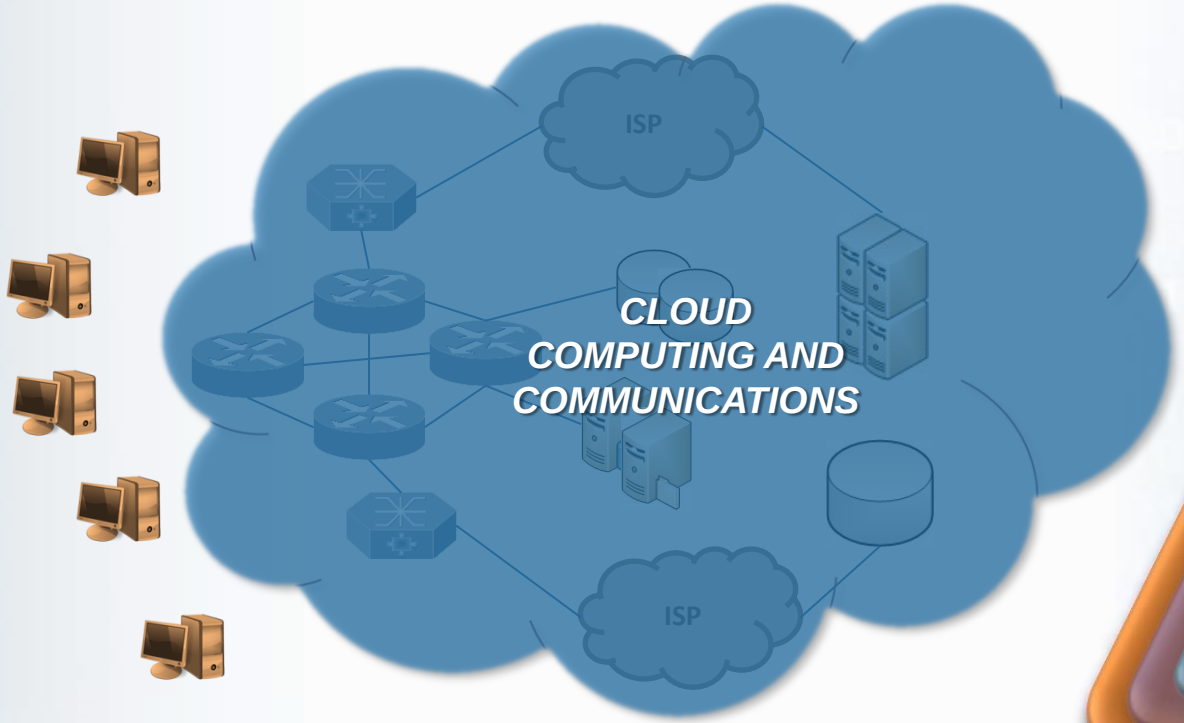
- The accelerated mutation of telcos from HW-based to SW-based
- The global interconnection and interdependence of critical information infrastructures
- The dawn of advanced persistent threats and target attacks for disruption, fraud and/or information collection

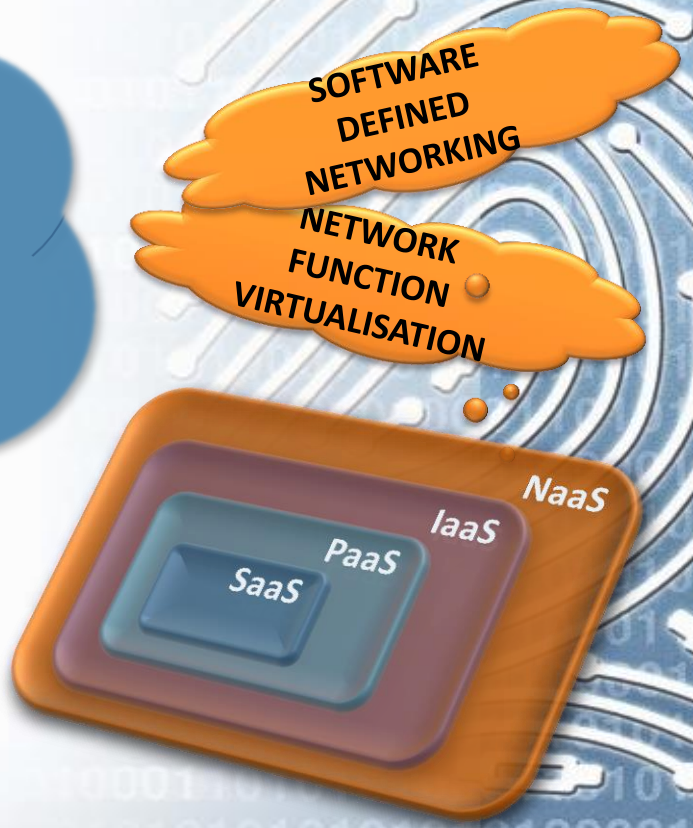
The phenomenal evolution of telcos from Comms to Comp

- to become distributed computer systems where the old core function (voice and data commuting) becomes embedded in a whole which is greater than the sum of the parts
- *"We (AT&T) are a software company."* [Andre Fuetsch, Senior VP of Architecture and Design at AT&T]
  - Internet/Cloud complex, Software-Defined Networking, Network Function Virtualisation
- using the right models is crucial for the stability and resilience of operation

Computing and communications are becoming pervasive commodities

"buying computing and communications as buying electricity"

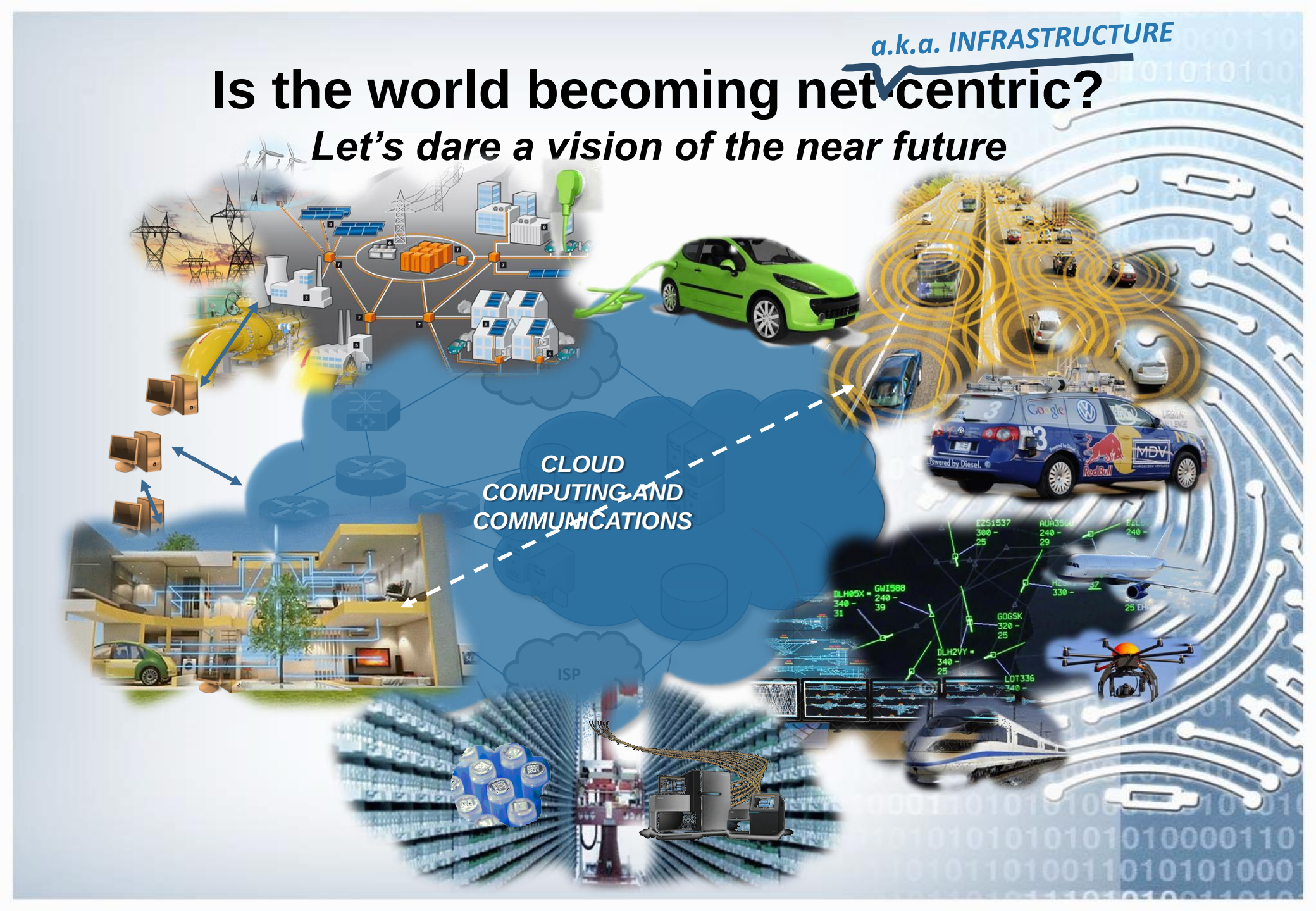




Is the world becoming net centric?

a.k.a. INFRASTRUCTURE

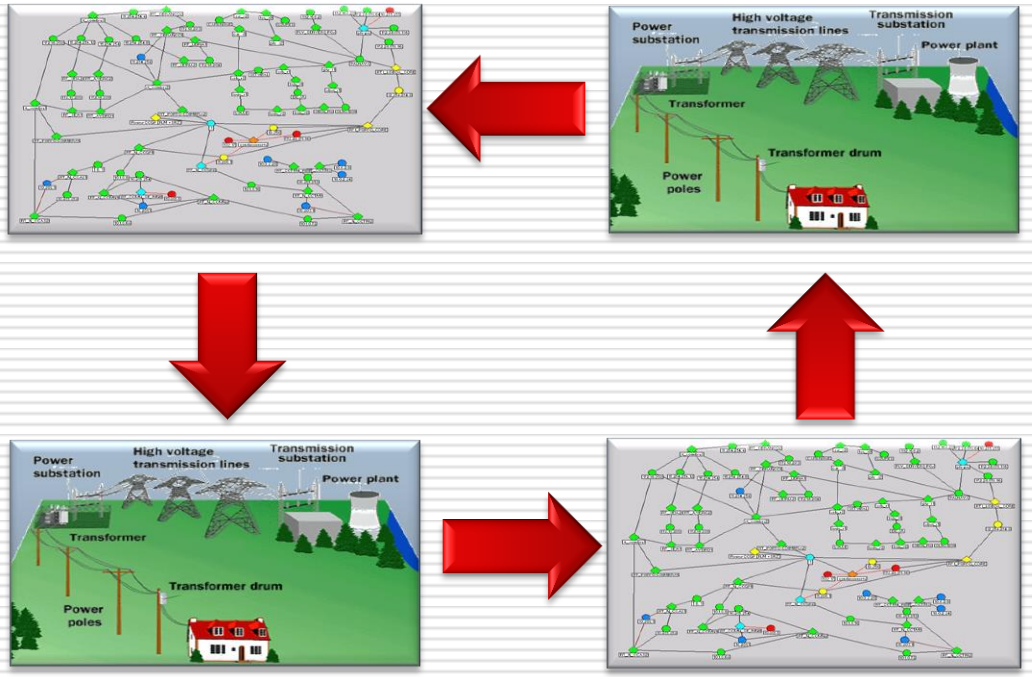
Let's dare a vision of the near future



An example of interdependence:

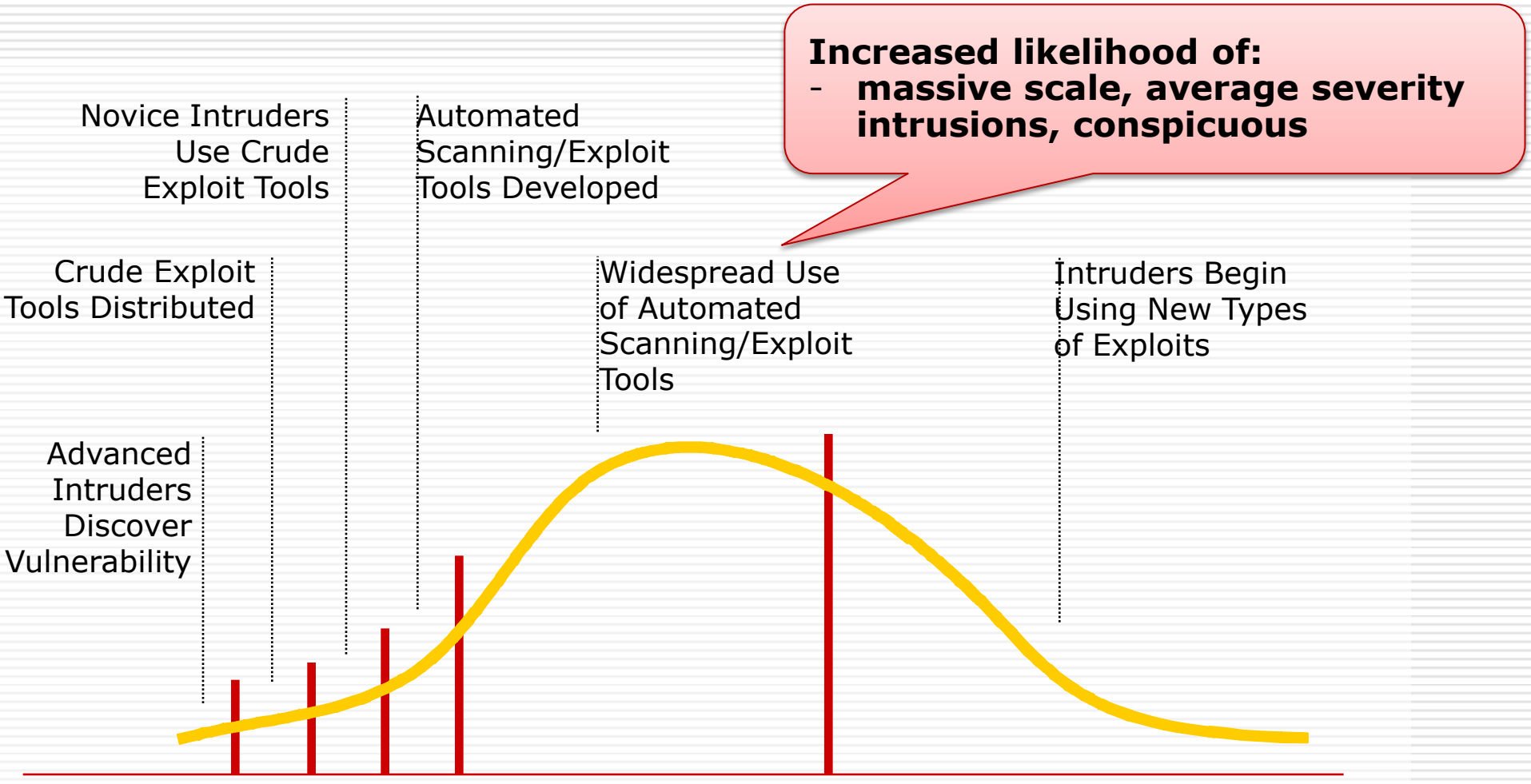
the power grid vs. the telecom network

- energy at the root of the infrastructures dependency hierarchy?
- not any longer...



Vulnerability Exploit Cycle

past and present



Threat Level

TechCrunch EUROPE

(Real) Storm Crushes Amazon Cloud, Knocks out Netflix, Pinterest, Instagram

BY ROBERT MCMILLAN 06.30.12 3:39 PM

Follow @bobmcmillan

Amazon EC2 goes Quora

by Mike Butch

Cloud comp

Reddit, Fou

morning, ac

Amazon says

"continuing t

1:48 AM P

2:16 AM P

region.

3:05 AM PI

US-EAST-1

4:03 AM PD

instance cre

European-based

Quora even has

lawfully se

But unkno

Amazon Cloud Crashes, Takes Part Of Web Offline

Submitted by Tyler Durden on 10/22/2012 16:28 -0400

Curious why there are those with an online business, who believe that handing over their entire back office infrastructure to one company, aka "going cloud" may not be the wisest of ideas. Just ask all those websites that use Amazon's cloud service today, who suddenly went dark when the Amazon cloud crashed.

Mike Miley

Jewson's employment for an allegedly logged back into his former

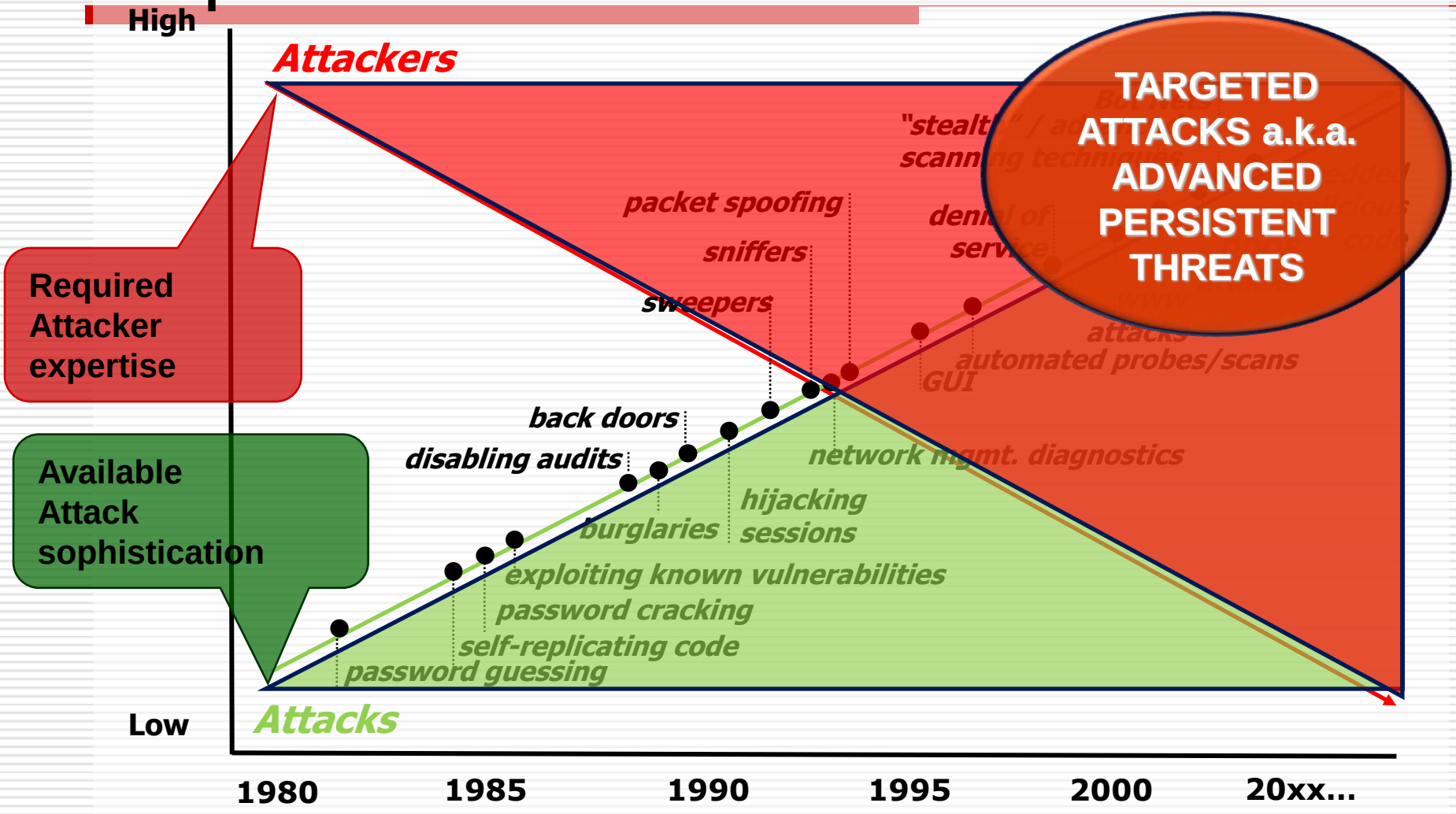
page.

reselling the inform

rds also

The era of DDoS Attacks

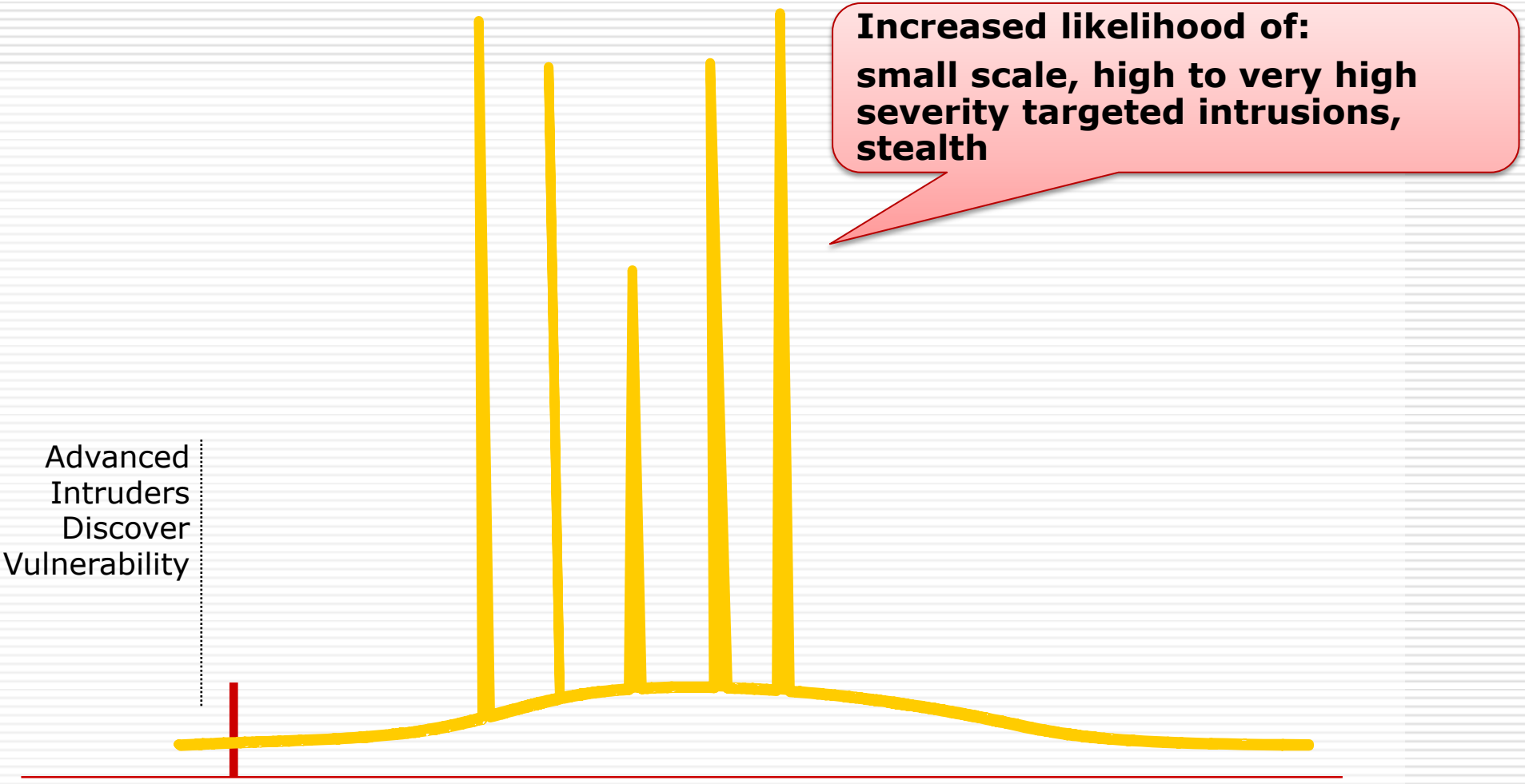
Attack sophistication vs. attacker expertise



(Source: Adapted from Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009, November 2002. (CERT)

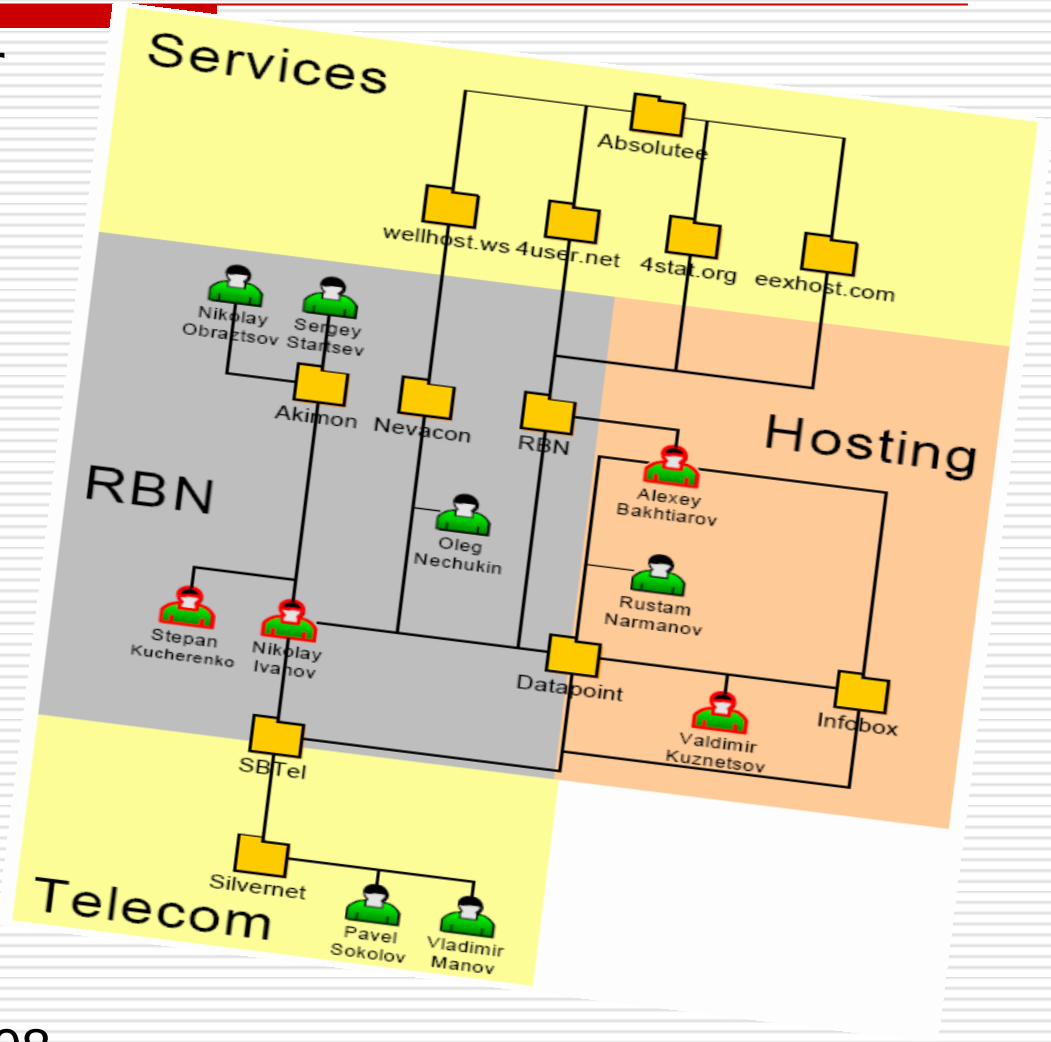
Vulnerability Exploit Cycle

present and future



Bullet-proof Networks
RBN – Russian Business Network

- **RBN:** core of RBN used to offer Hosting for cybercrime (Nevacon and Akimon)
- **Hosting:** used to host most of RBN public websites, register RBN domain names
- **Telecom:** aims at providing the Internet access for RBN (SBTel - Silvernet -SPBIX).
- **Services:** external services used by RBN and affiliates. (ex. MX relay or NS hosting)



David Bizeul, RBN Study, 2008

MANDIANT

THREAT LANDSCAPE

Mandiant Exposes APT1 – One of China's Cyber Units & Releases 3,000 Indicators

By Dan Mcwhorter on February 18, 2013

Today, The Mandiant® Intelligence Center™ released an unprecedented multi-year, enterprise-scale computer espionage campaign. APT1 is one Mandiant tracks around the world and we consider it to be one of the mos quantity of information it has stolen.

SPIEGEL ONLINE INTERNATIONAL

Sign in | Register

Front Page | World | Europe | Germany | Business | Zeitgeist | Newsletter

English Site > World > NSA Spying Scandal > The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks

Inside TAO: Documents Reveal Top NSA Hacking Unit

By SPIEGEL Staff

iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign

By Stephen Ward October 14, 2014 iSIGHT Partners

RISK ASSESSM

Report: NSA paid RSA to ma algorithm the default

The NSA apparently paid RSA $10M to use Dual EC

by **Peter Bright** - Dec 20 2013, 11:14pm GMTDT

SandWorm

Zero-day impacting all versions of Microsoft Windows – used in Russian cyber-espionage campaign targeting NATO, European Union, Telecommunications and Energy sectors

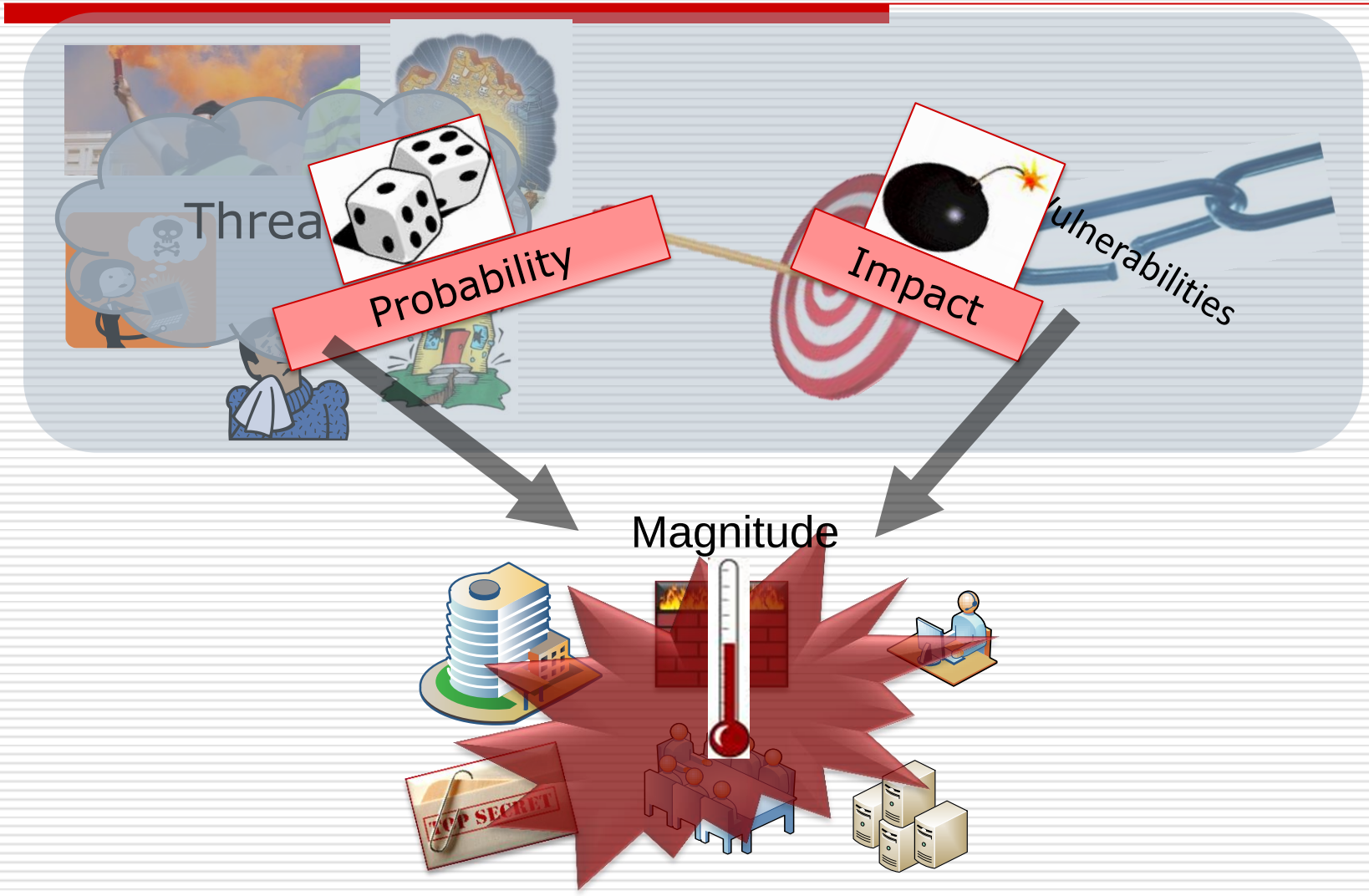
uni.lu UNIVERSITÉ DU LUXEMBOURG

The road to resilience

… a necessary "OPS" and Regulators perspective …

Understanding risk

Understanding risk



Assessing risk
Risk analysis objectives

- Identifying and evaluating the main risks, of different natures, impending over national Telco/Internet/Cloud complex infrastructures
- In more detail:

  analysing the level of threat, considering reference scenarios;

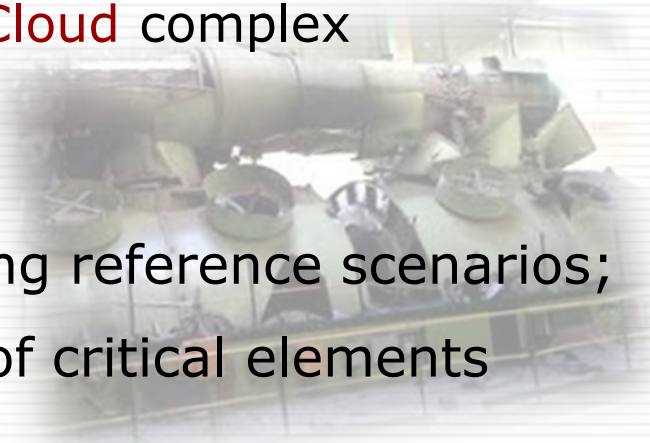
  identifying the degree of vulnerability of critical elements

  evaluating the risk on critical elements

  aggregating results: elements -> OPS -> national

  evaluating the maturity of the systems

  presenting recommendations for risk mitigation and maturity enhancement



Assessing risk
Metrics – Risk Analysis matrix

RISK MAGNITUDE DEFINITION TABLE (as f(Impact, Probability))

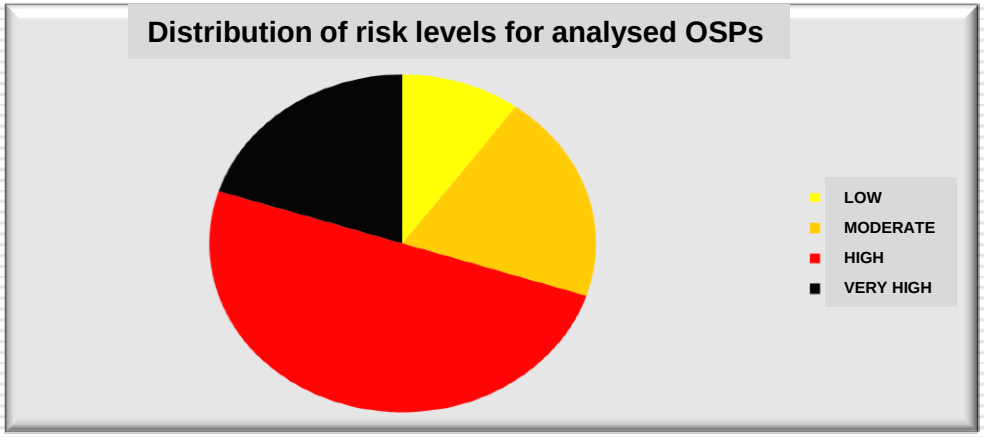
Impact	VERY HIGH	MODERATE	HIGH	VERY HIGH	VERY HIGH
	HIGH	MODERATE	HIGH	HIGH	HIGH
	MODERATE	LOW	MODERATE	MODERATE	MODERATE
	LOW	LOW	LOW	LOW	LOW
0,6667		LOW	MODERATE	HIGH	VERY HIGH
	0,3333	**Probability (Level of threat x degree of vulnerability)**			

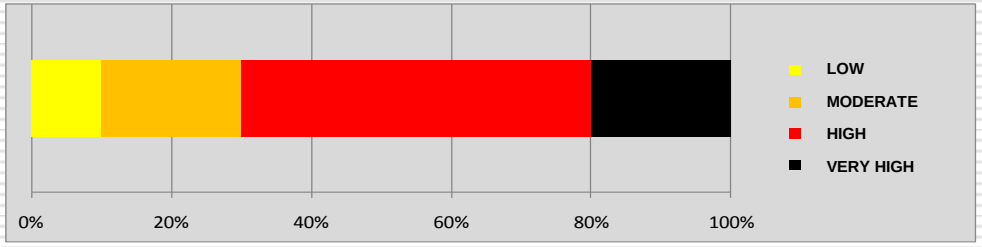
Computed for every critical element and OSP

Assessing risk

Example diagnosis – Risk of a national system

- Example diagnosis and distribution of risk levels for a national system in a reference scenario





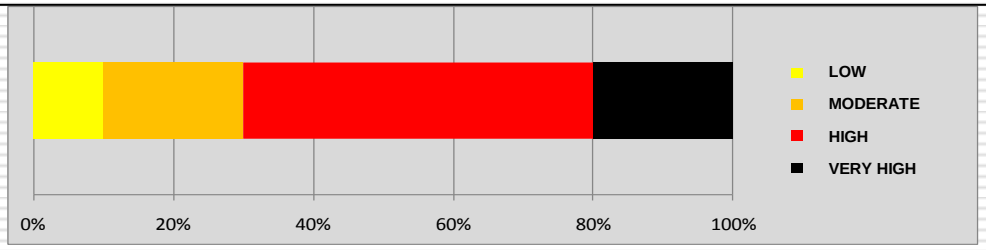
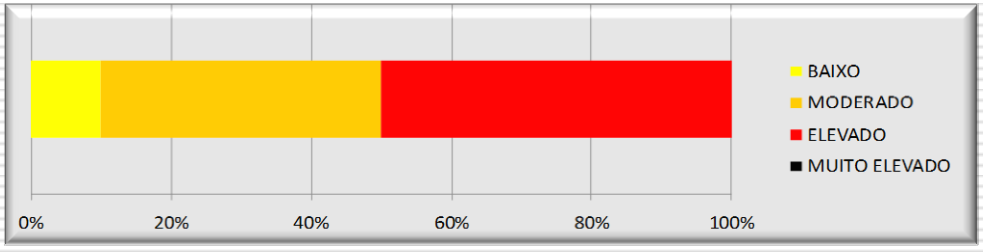
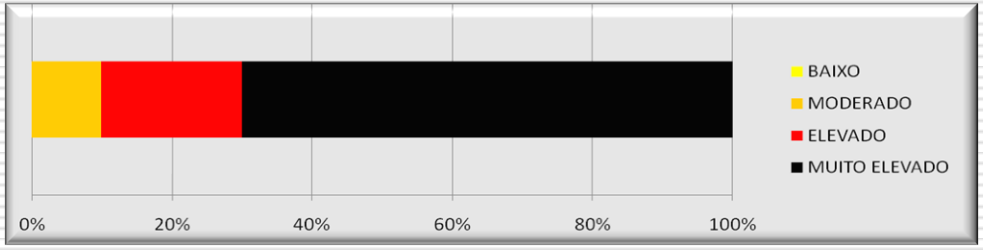
National Risk

HIGH

Assessing risk

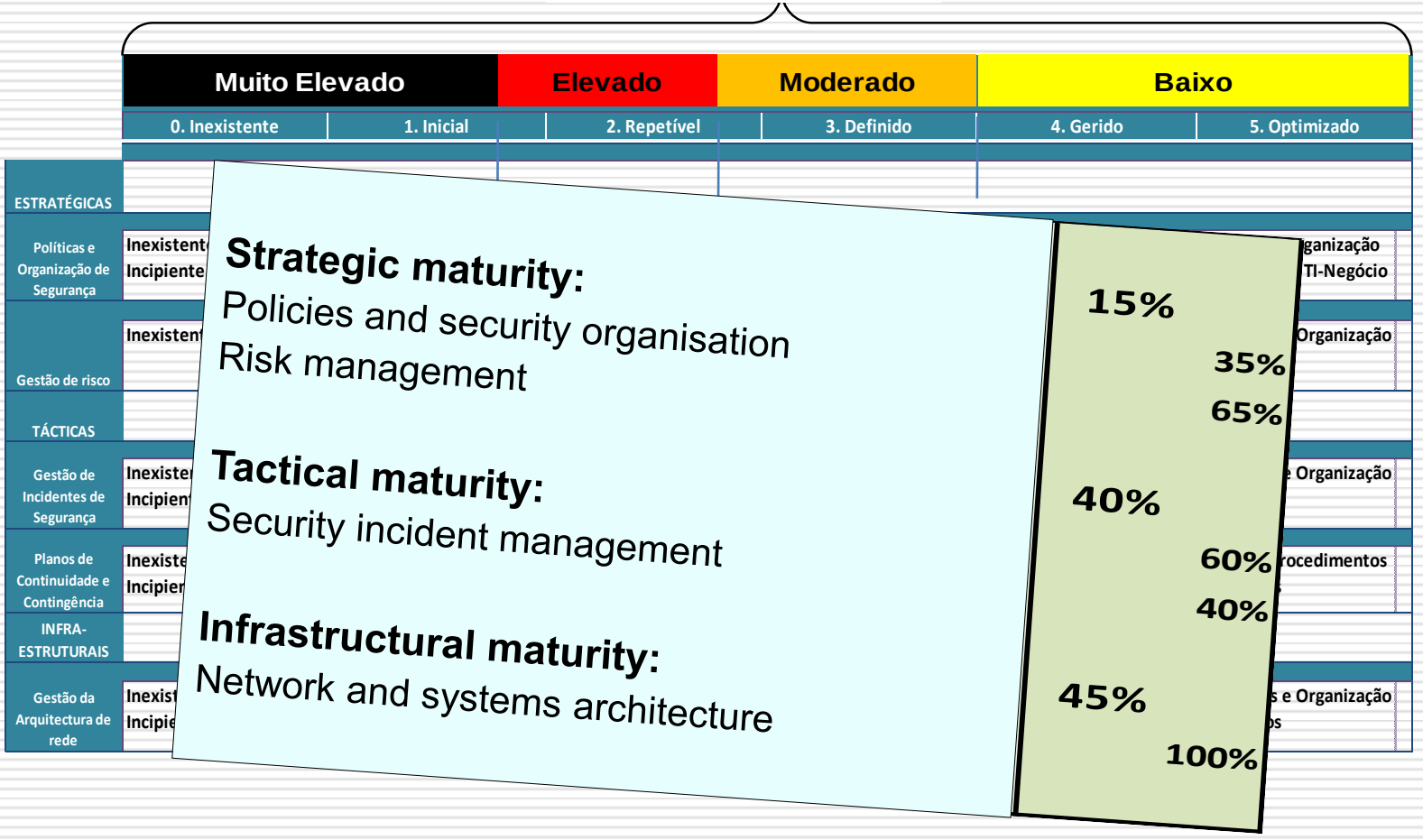
Example diagnosis – Risk of a national system

- Example diagnosis and distribution of risk levels for a national system in multiple scenarios: reference, moderate, enhanced threats

Threat Scenario	Distribution of risk levels	National Risk
COMBINED		HIGH
MODERATE		MODERATE
ENHANCED		VERY HIGH

Assessing risk
Evaluating maturity of a national system

- *Example evaluation* of maturity along several axes, from technical to organisational



Assessing risk
Testing infrastructure resilience

- Combined exercise in ciberdefense and cybersecurity, Portugal

Is resilience really necessary?

- Adm. Michael Rogers, NSA Director and commander of US Cyber Command, said that the question "How, in the midst of degradation and penetration, can we still have confidence in the systems?" is better served by ***focusing on resilience rather than on prevention***.
- [Editor's Note]: This is the new theme for cybersecurity - the ability to ***continue fighting when you're hurt*** is the differentiator between a successful security organization and the one picking up the pieces after an incident and wondering what happened.

FEDERAL TIMES
A GANNETT COMPANY

Print: Subscribe Renew Digital Edition MOBILITY CYBER FEDERA

Sign up for our free newsletters

IT security shifts from prevention to resiliency

Sep. 22, 2014 - 06:00AM | By AARON BOYD | Comments

Recommend 31 Pin it

Adm. Michael Rogers: Preventing or stopping intruders is only half of the equation for maintaining resiliency. (Mark Wilson/Getty Images)

The discussion on cybersecurity has shifted as CIOs and CTOs come to the realization that no system is immune to attacks and breaches. The conversation is now about "cyber resiliency."

"How, in the midst of degradation and penetration, can we still have confidence in the systems?" Adm. Michael Rogers, NSA director and commander of U.S. Cyber Command, asked at the Billington Cybersecurity Summit in Washington. "Most organizations have tended to put their resources and focus on stopping people from penetrating their systems. I tell organizations that we have got to not only focus on stopping people... but how are you going to operate and remediate at the same time. That's resiliency."

But will really bad things happen to CII?

- [several] ***countries have the capacity to shut down nation's … critical infrastruct. through a cyber attack***». [Adm. Michael Rogers, NSA Director and commander of US Cyber Command]
- … a recent prediction by technology experts says that a catastrophic cyber-attack that causes significant losses in life and financial damage would occur by 2025.
- "It is only ***a matter of the when, not the if, that we are going to see something traumatic***." [Ibid.]

The U.S. government thinks China could take down the power grid

By **Jamie Crawford**, National Security Producer
November 21, 2014 -- Updated 2319 GMT (0719 HKT)

Click to play

Could China cripple U.S. power grid?

STORY HIGHLIGHTS

- The head of U.S. Cyber Command said China has the ability to attack the U.S. power grid

Washington (CNN) -- China and "probably one or two other" countries have the capacity to shut down the nation's power grid and other critical infrastructure through a cyber attack, the head of the National Security Agency told a Congressional panel Thursday.

Some conclusions

- Threat and vulnerability landscape has dark clouds
- Telcos are IT companies, it is not just comm's, and the Telco/ Internet/Cloud complex is a most critical infrastructure
- It is imperative for a nation to evaluate the criticality and risk those systems offer to the activity supported: regular audits, transparency, improvement
- Regulations (EC) about IT, Telco and CI related hazards are in line with this status quo
- IT/Telco and CII strategists must assess the respective level of trustworthiness and resilience, and improve it to target levels
- First enhancement to maturity is knowing your weaknesses
- For CIIs, "security" is not enough, you need "best security" and this implies companies as well as governments: best practices and technologies; best personnel to bring them into action

Thank you!

Paulo Esteves Veríssimo, ***CRITIX*** @SnT, paulo.verissimo@uni.lu