Towards a general theory of resilience. Lessons from a multi-perspective research.

Paul Théron

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

Towards a general theory of resilience. Lessons from a multi-perspective research.

ERNCIP lecture, Brussels, 22/06/2016

Paul THERON, PhD, FBCI

crest.researchgroup@gmail.com

Introducing myself briefly

Thales Communications & Security

- Cyber defence bid manager (Export)
- (Cyber) Resilience expert

Co-Head of the French "Aero spatial cyber resilience" research chair

- Founders: French Air Force + Thales + Dassault Aviation
- Interdisciplinary: Multi Agent Cyber Defence, Cognition, Engineering

My research: Toward a "general theory of resilience"?

- Individual cognition and peritraumatic resilience
- Systems' (cyber) resilience
- Resilience of work collectives / Teams
- Corporate resilience
- Critical infrastructures' resilience
- Multilevel governance of critical infrastructure resilience

CREST (Crises & Resilience – Economy, Society, Technology) is an independent research group.

It promotes interdisciplinary, multi perspective research on resilience.

Its object is the dynamics of resilience at the *pre*, *peri* and *post* incident stages.

It was started in 2006 as CREST (Cognition – Resilience – Trauma) and initiated the PhenoCognitive Analysis of individual cognition in action & peritraumatic resilience: https://sites.google.com/site/cognitionresiliencetrauma/home

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

Question to the class

Resilience is / can be defined as…

- Tour de table

Question to the class

We talk so much about resilience these days because…

- Tour de table

Agenda

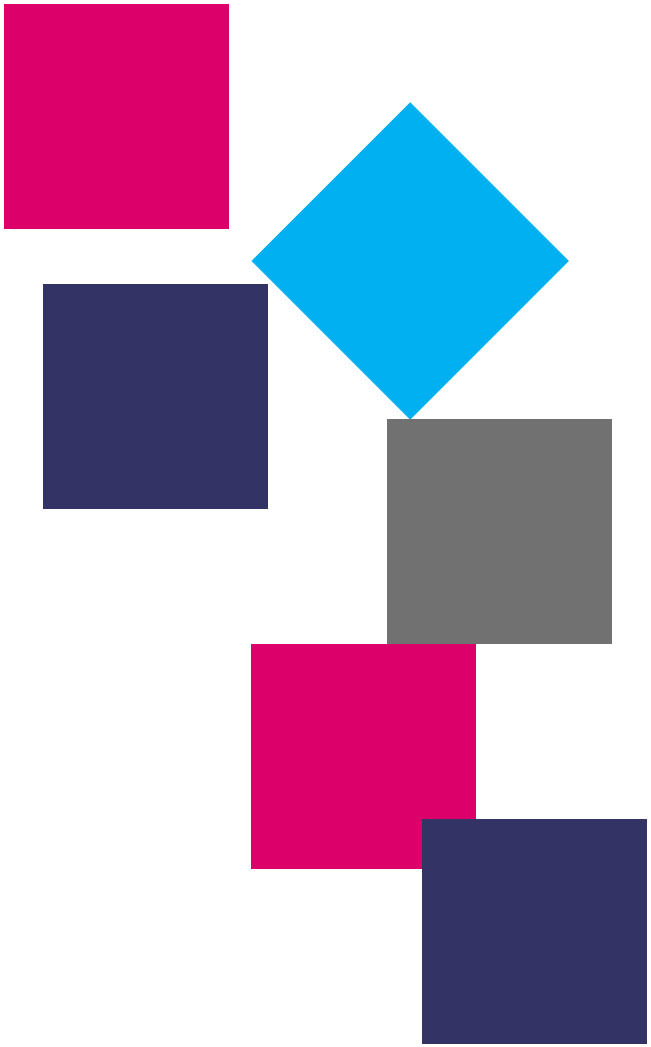
What is resilience?

Governing resilience in the context of critical infrastructures

Conclusions

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

What is resilience?

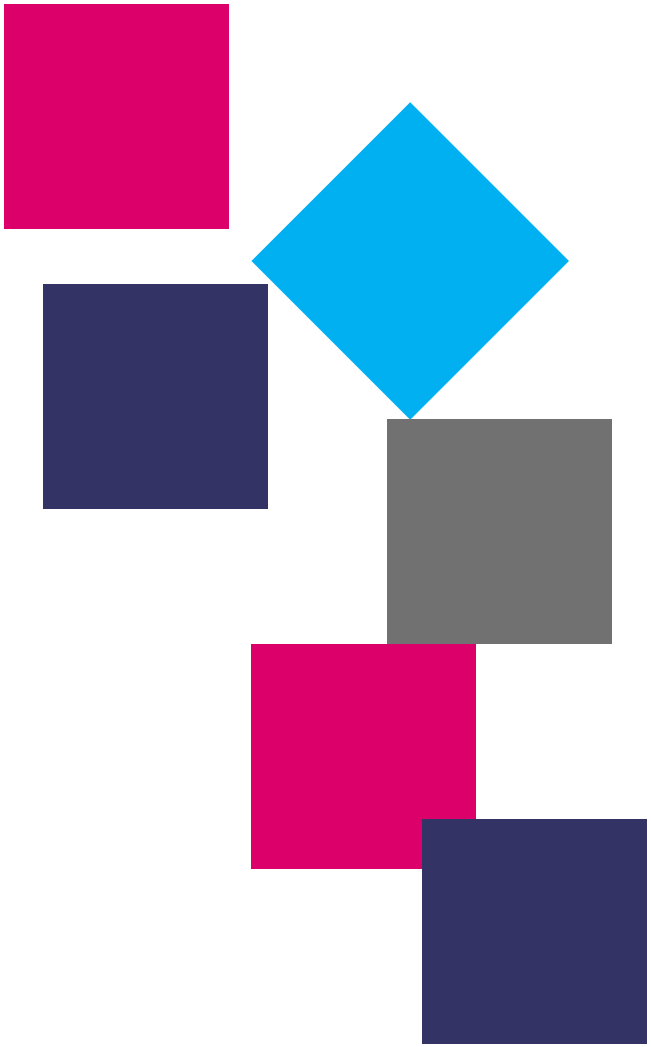


crest.researchgroup@gmail.com

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

Case studies all point to a common phenomenon…

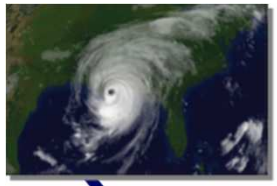
Resilience is a struggle against collapse



crest.researchgroup@gmail.com

Collapse in New-Orleans (Katrina, August 2005)

Preparing for the expected



Alarm

Evacuation

Refuge

Last precautions

Shock

Devastation

THERON – OPEN

Survival

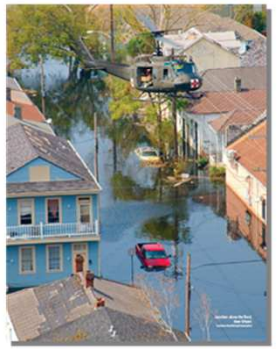
Preparation of rescue

Déployment

Incidents

Security restauration

After-shock



Fighting unexpectedness

CRISES & RESILIENCE ECONOMY TECHNOLOGY CREST SOCIETY

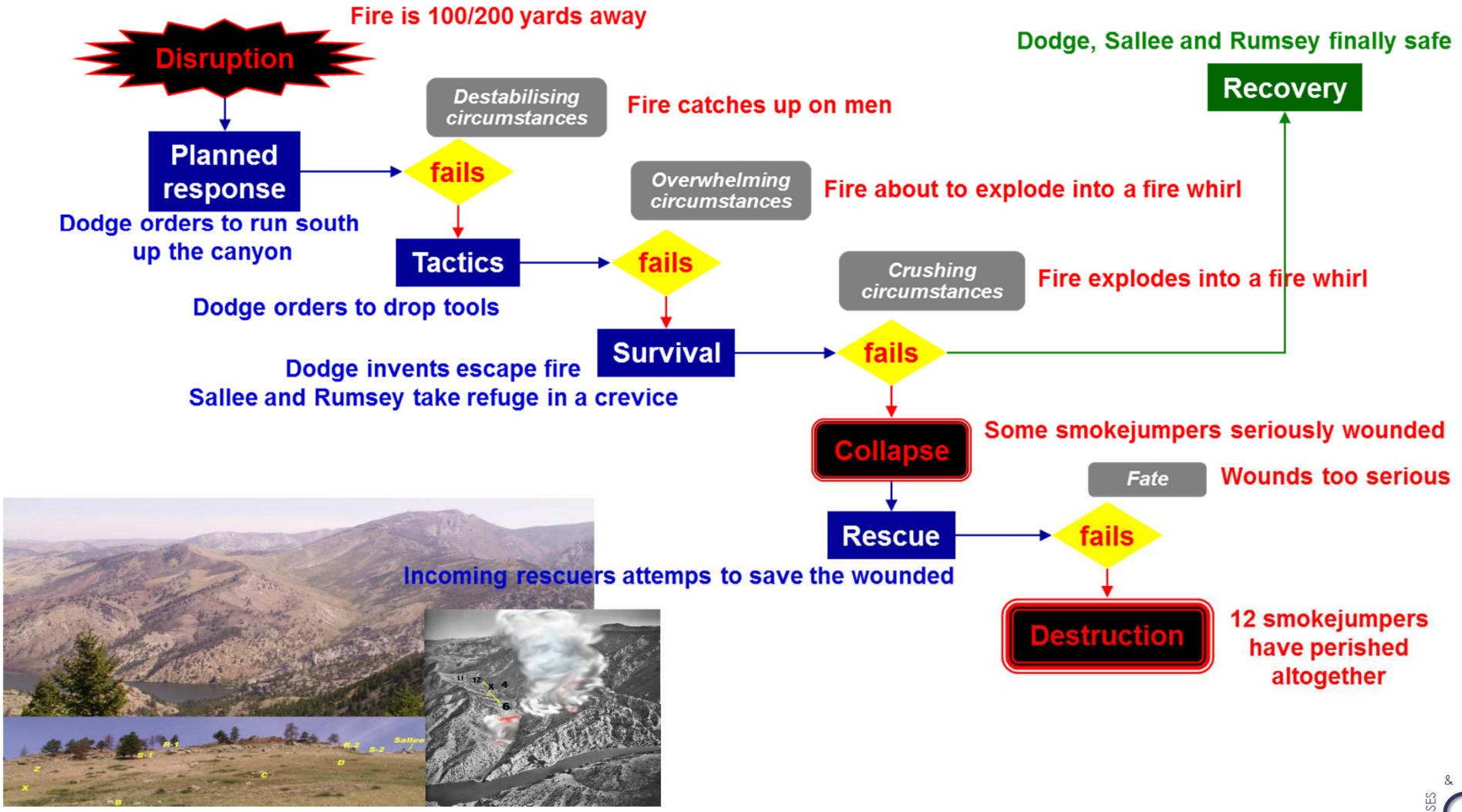
Collapse of News of the World (Summer 2011)

Couldn't regain control of CoE*…

So terminated NOTW

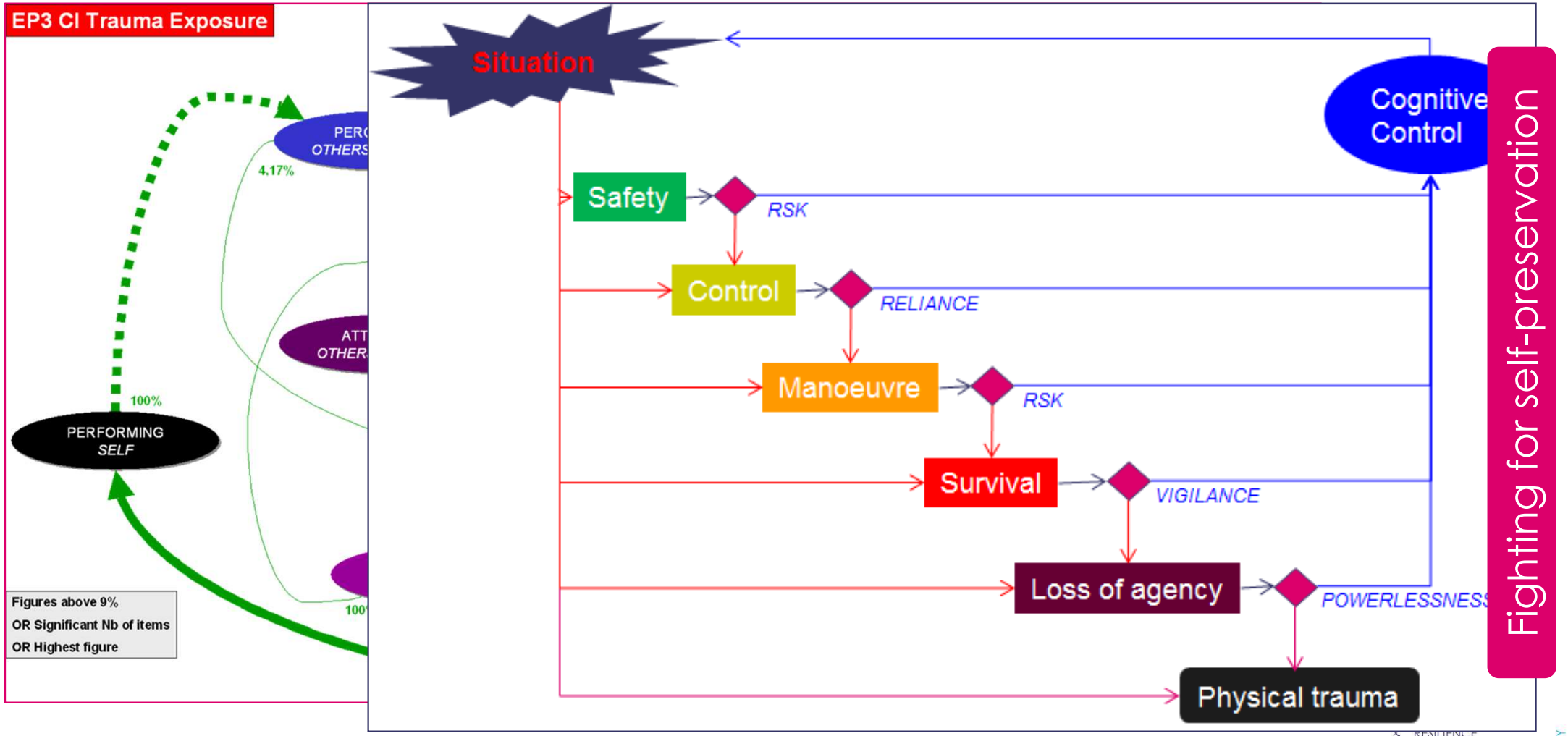
* Course of Events

Collapse at Mann Gulch (August 1949, USA, Montana)



Adapting to growing pressure

Lieutenant A & the rottweilers: a cognitive struggle for safety

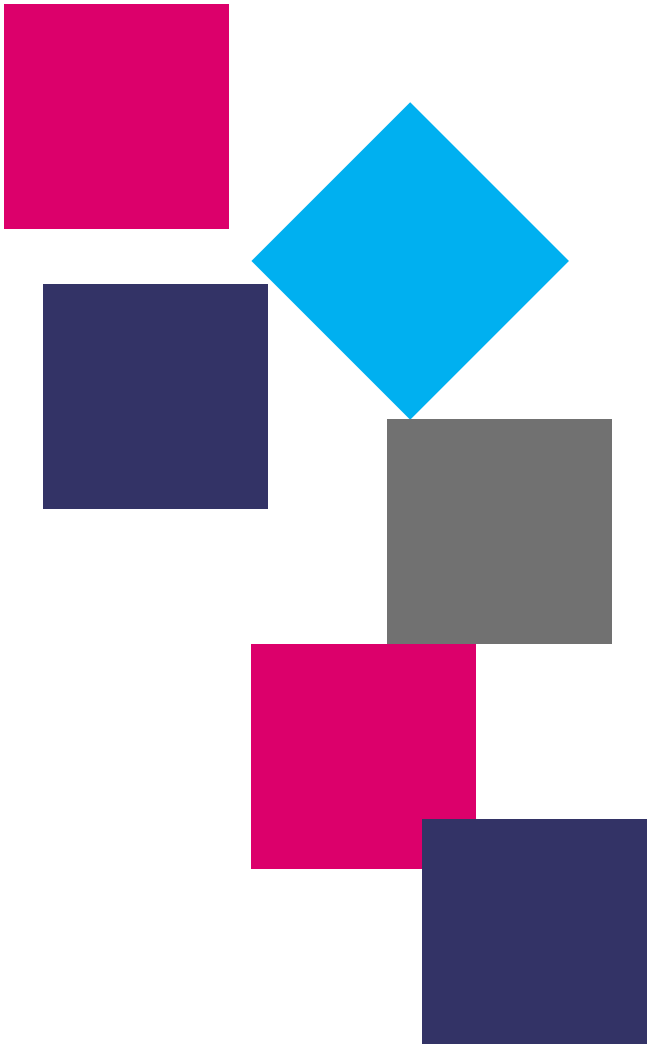


http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.616373

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

Recent techno-focused literature too…

Resilience is confirmed to be a struggle against collapse



crest.researchgroup@gmail.com

Sources studied (as of end of 2011)

- EC COM(2009)149
- ENISA (2010) Gaps in standardisation related to resilience of communication networks
- ETSI TR 102 445 Emergency Communications (EMTEL): Overview of Emergency Communications Network Resilience and Preparedness
- ENISA (2011) Ontology and taxonomies of resilience (DRAFT)
- ENISA (2011) Inter-X: Resilience of the Internet Interconnection Ecosystem
- Survivability (Sterbenz et al., 2010)
- ENISA (2011) Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report (Draft)
- EC - JLS/2008/D1/018 : A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet

ENISA (2011) Inter-X: Resilience of the Internet Interconnection Ecosystem

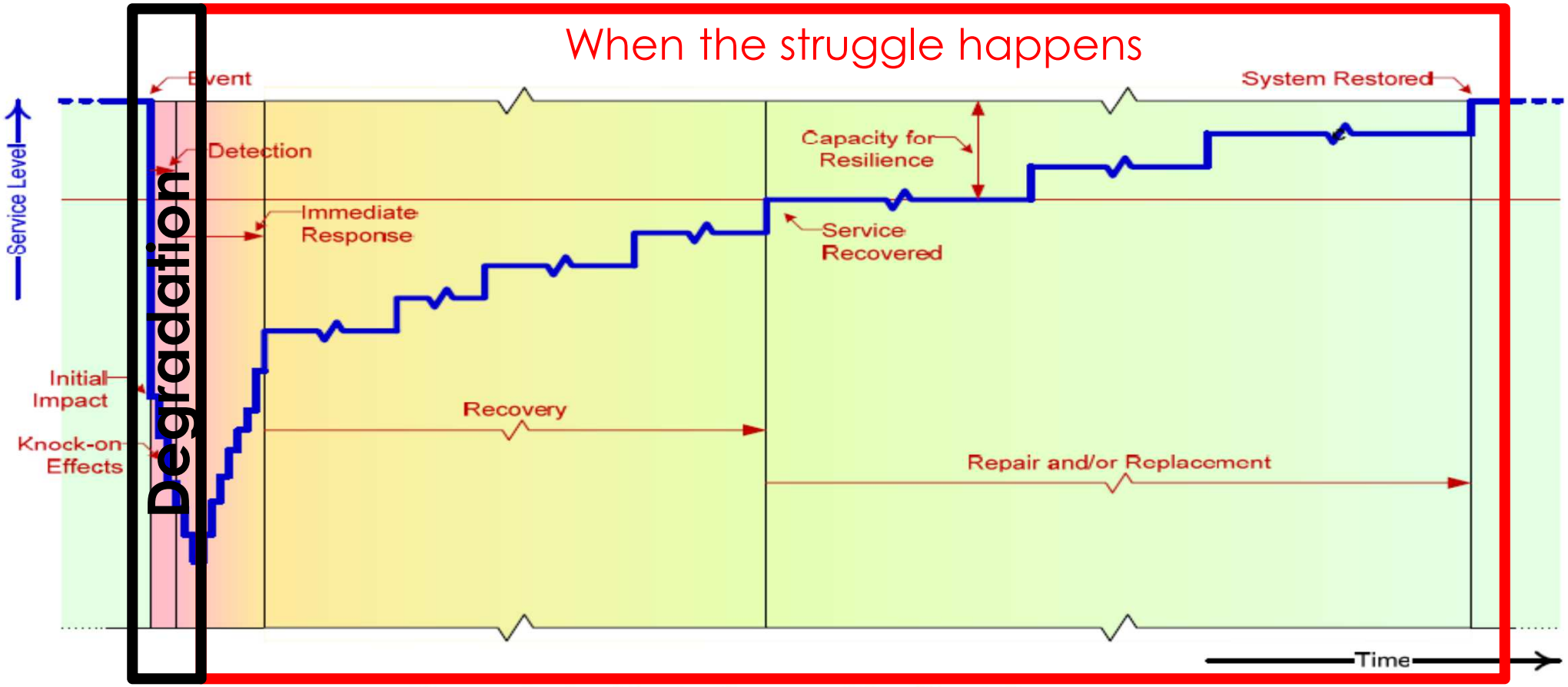
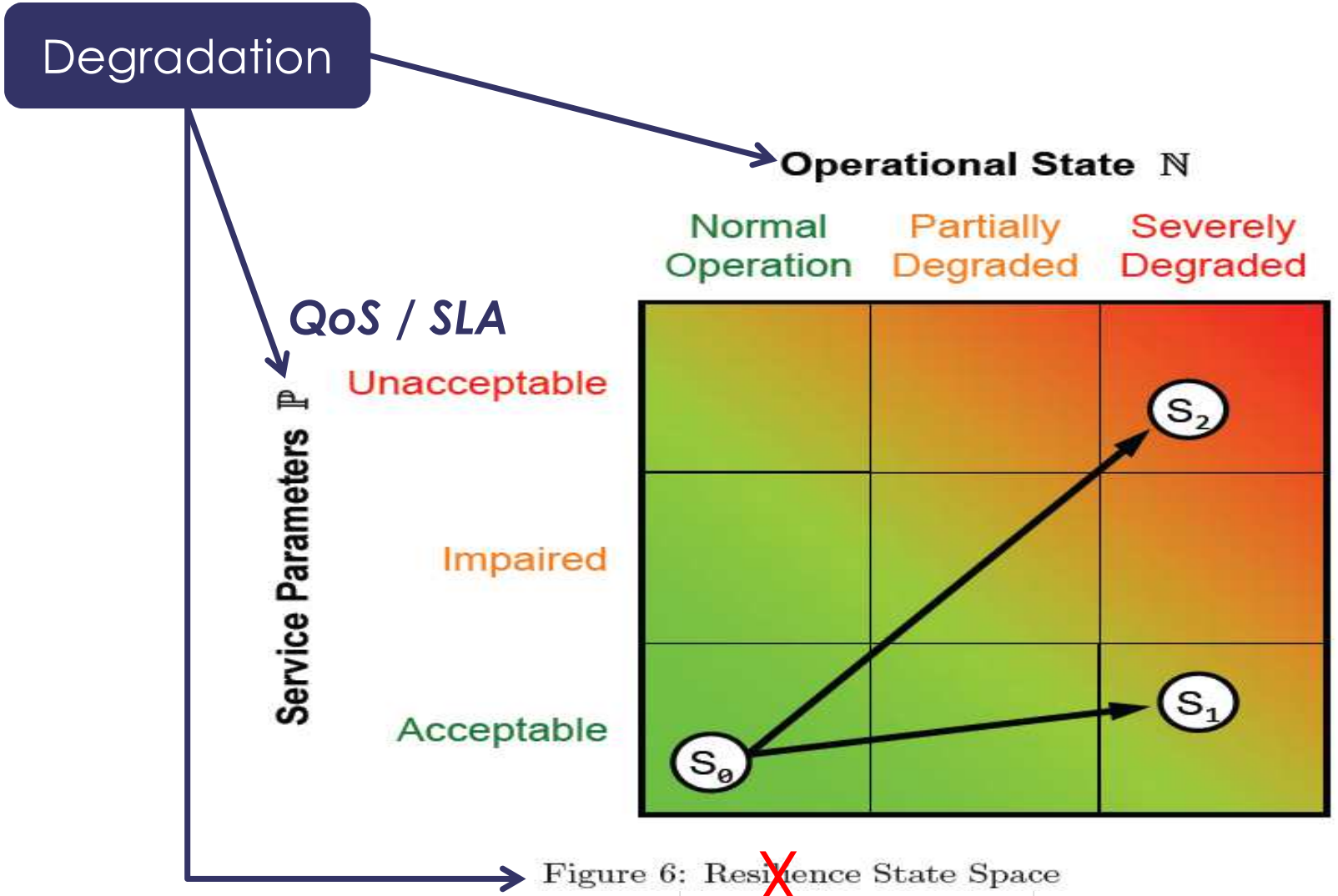


Figure An Incident: Phases of Resilient Response

Survivability (Sterbenz & al., 2010)



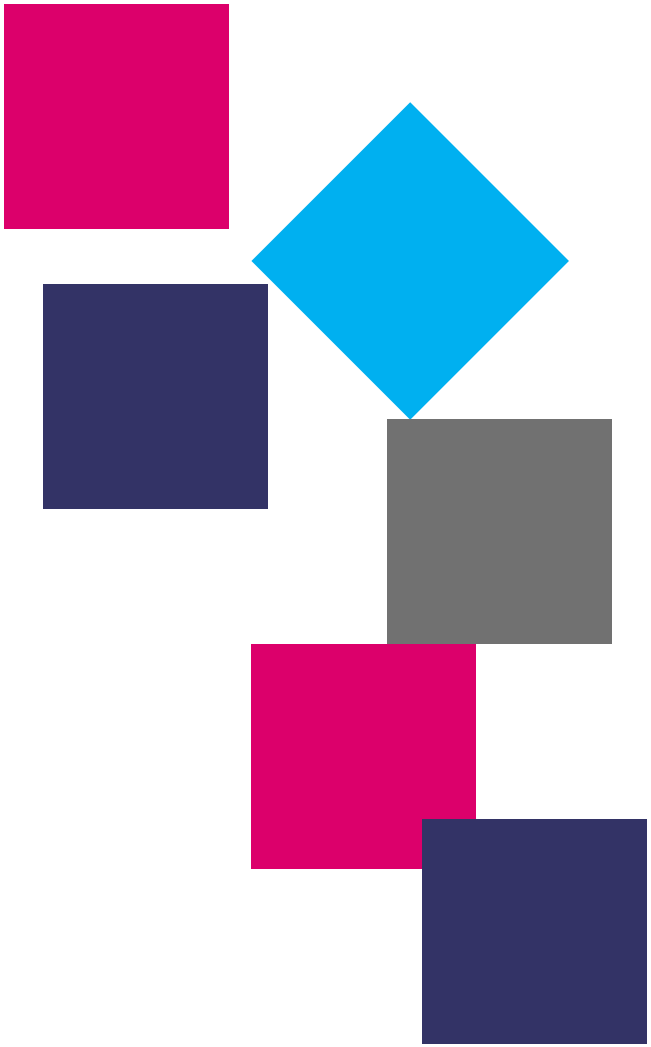
Integrity / State of collapse

Figure 6: Resilience State Space

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

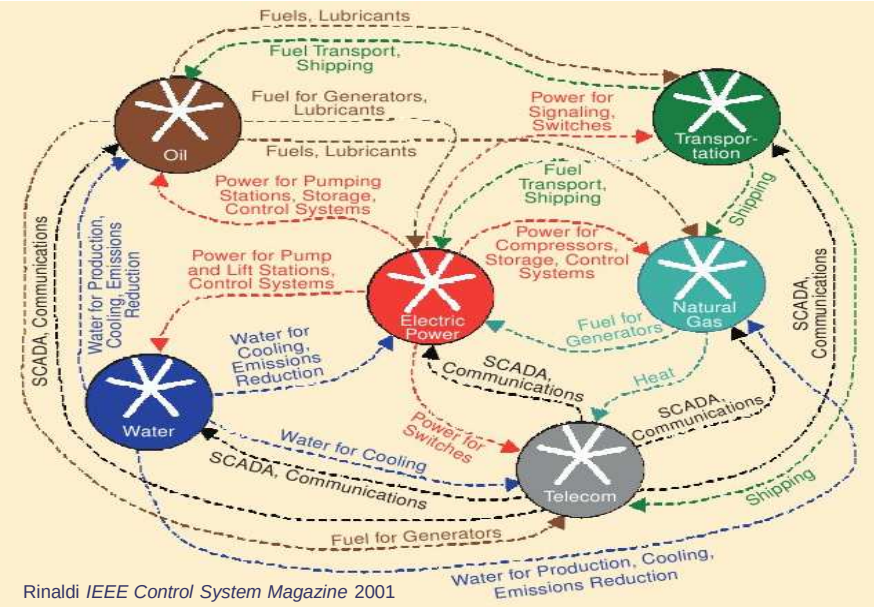
A definition of resilience

7 findings & precepts about resilience



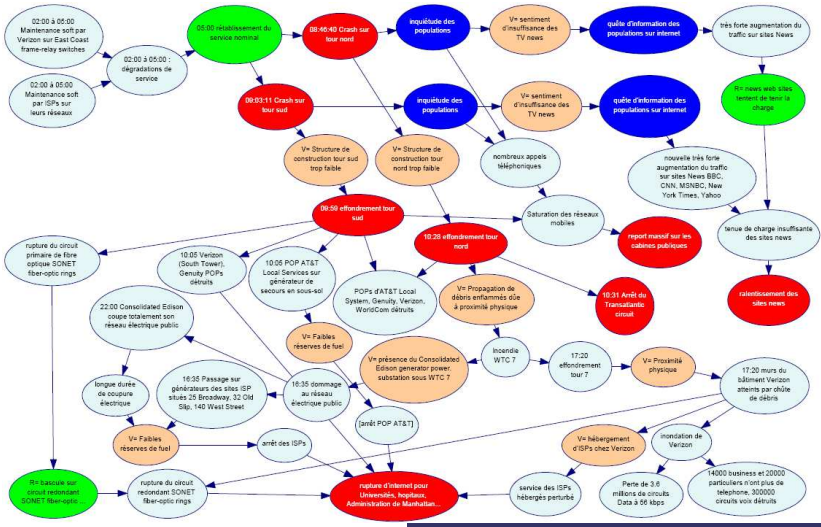
crest.researchgroup@gmail.com

1st finding: why it is needed (Accept that complexity will defeat you)

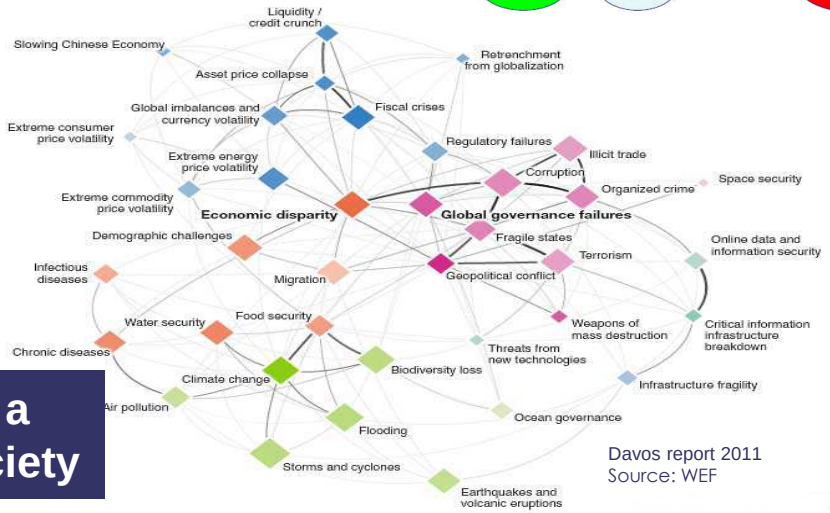


Rinaldi *IEEE Control System Magazine* 2001

Complexity stemming from interdependencies



Complexity of accidentogenesis

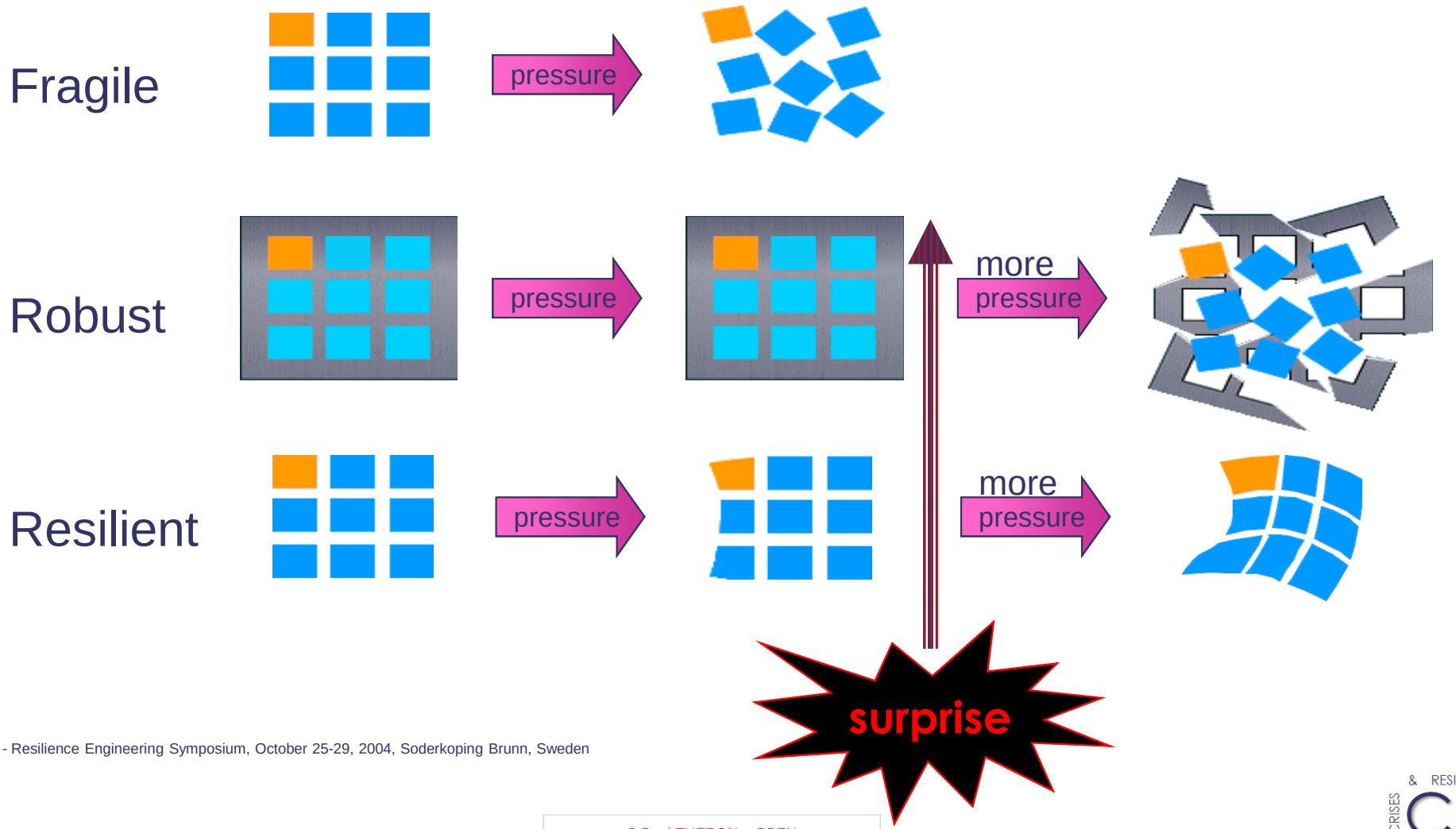


Davos report 2011
Source: WEF

Complexity of a crisis-prone society

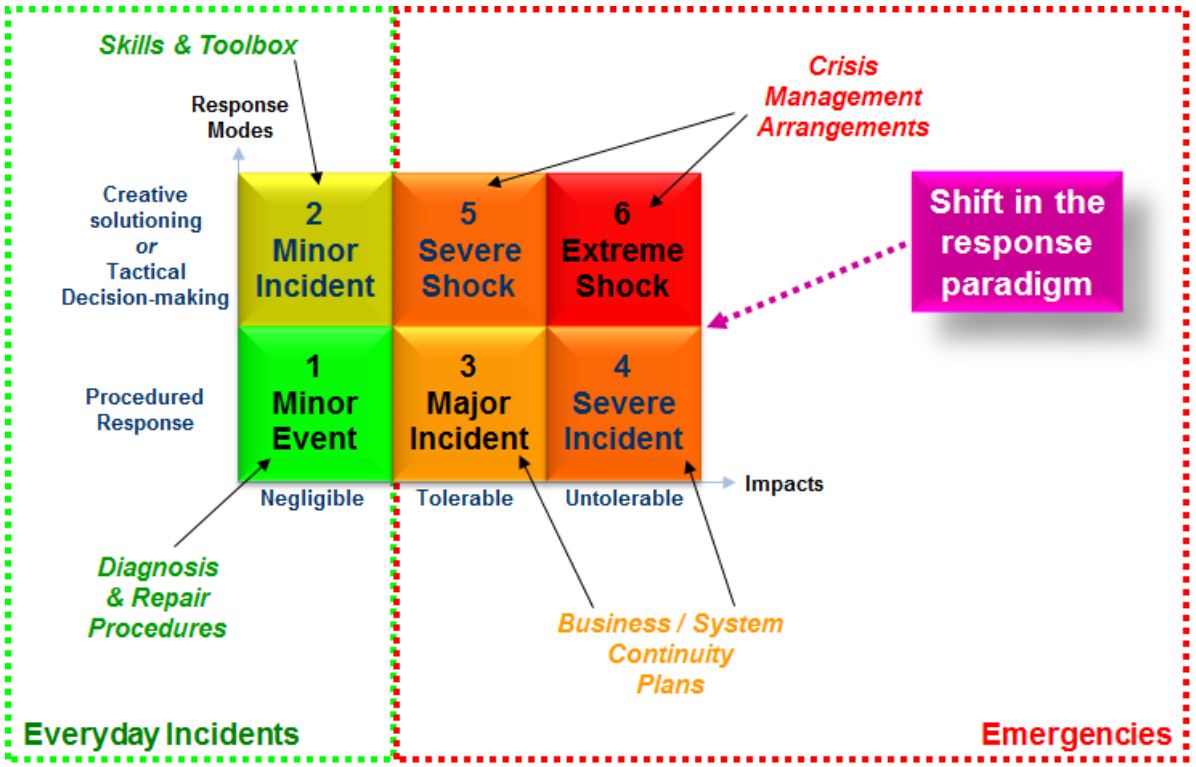
CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

2nd finding: why it is so misunderstood (Think beyond words)



Yushi Fujita - Resilience Engineering Symposium, October 25-29, 2004, Soderkoping Brunn, Sweden

3rd finding: what it helps to overcome (Set performance goals)



The Incident Severity Scale

Théron, P. (2013)

4th finding: how it can be defined (Explain your policy)

A crisis is an experience of collapse

- Of a socio-technical system
- Under the effect of a major shock
  - Surprising
  - Destabilising
  - Frightening

Resilience is the aptitude of a socio-technical system to surmount crises

- But this is an "extremist" standpoint…
  - Every step counts even modest ones
  - Cumulative Engineering delivers resilience

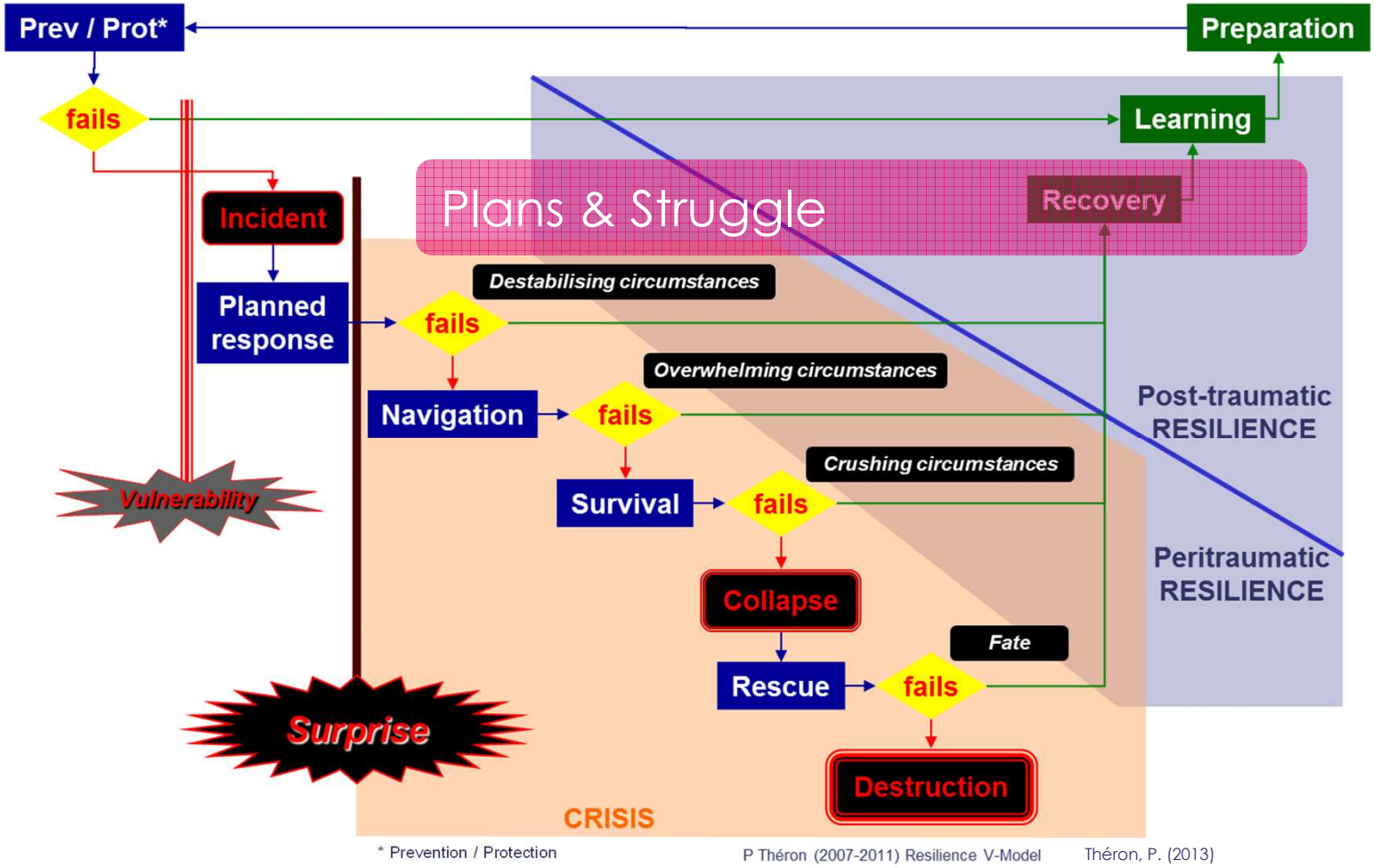
Resilience is the ability of a sociotechnical system

- Made of interacting human, technical and physical agents
- To surmount (together) adverse events, from mere incidents up to extreme shocks…

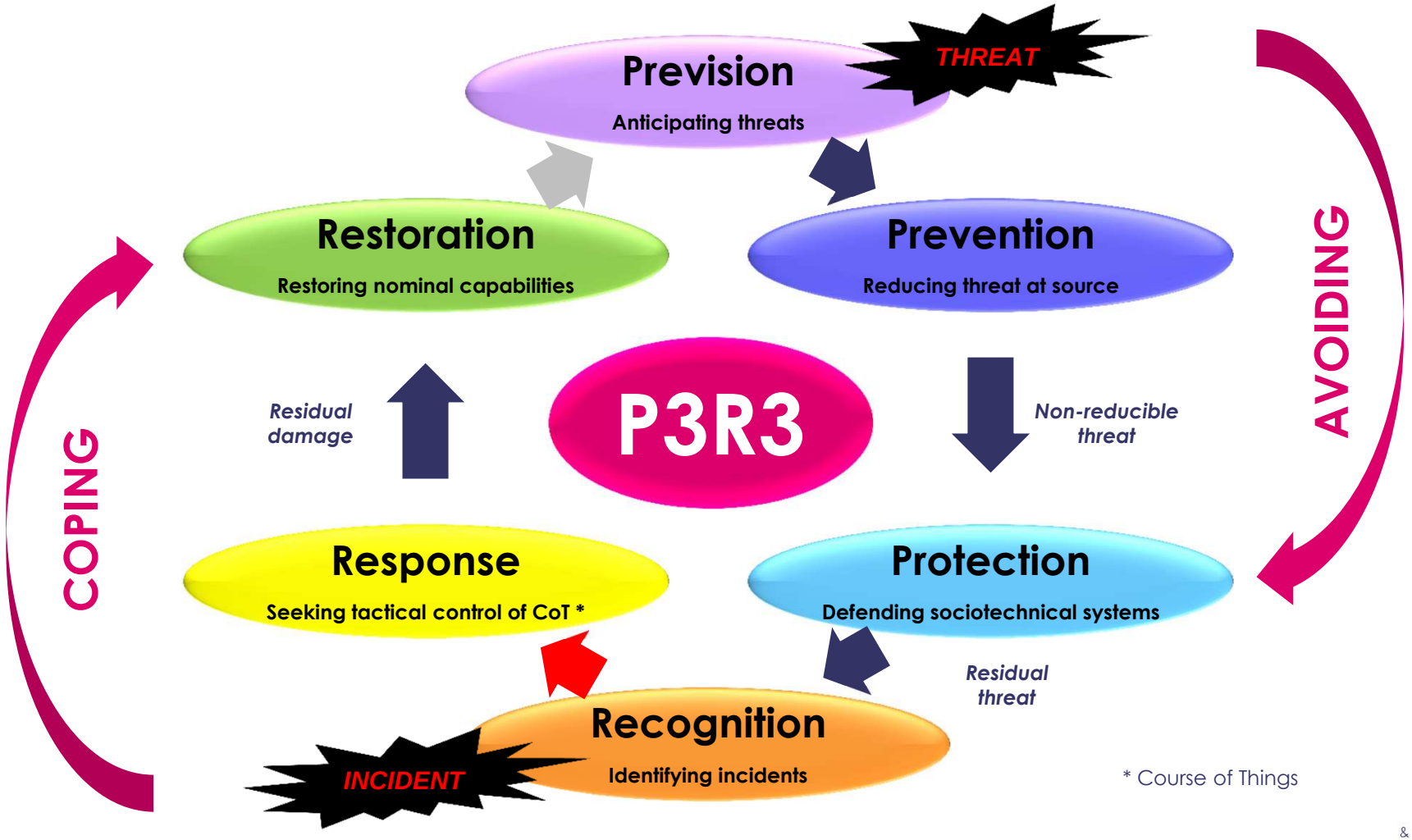
… through 5 activities to be run by all and for all

- Pre-incident = before incidents happen
  - Engineering : the system is built to avoid and resist expectable challenges, and to stand unexpectedness
- Peri-incident = while incidents are happening
  - Maintaining : the system finds ways to keep acting on its missions despite adversity
  - Resisting : the system finds ways to avoid collapsing and its possible destruction
  - Recovering : the system finds ways to return to a nominal course of life as soon as possible
- Post-incident = after incidents have happened
  - Rebounding : the system learns from and adapts to circumstances

5th finding: when it takes place (Prepare to fight)

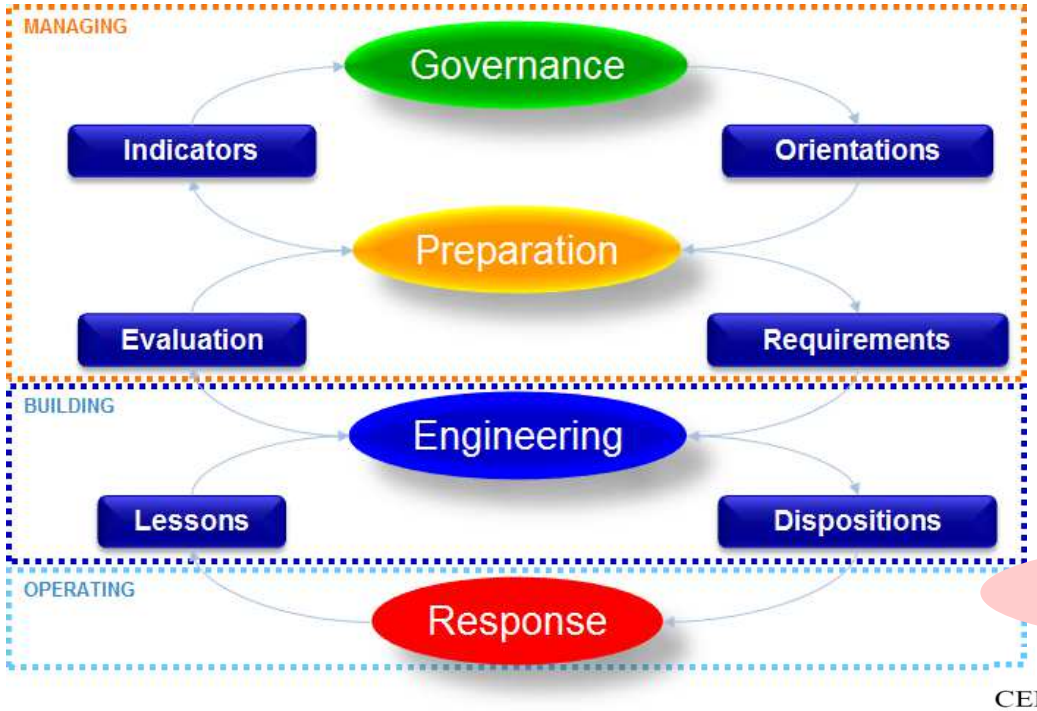


6th finding: what mechanisms engineering delivers (Act upon threats)



* Course of Things

7th finding: how it is governed (Prepare to collaborate)



INTERNATIONAL STANDARD **ISO 22313**

First edition
2012-12-15

Societal security — Business continuity management systems — Guidance

STANDARDISATION

GOVERNMENTS

Guidelines

Certification

STAKEHOLDERS

Software Engineering Institute

CERT® Resilience Management Model, Version 1.0

Process Areas, Generic Goals and Practices, and Glossary

LiU-ITN-TEK-G--13/072--SE

Linköpings universitet
TEKNISKA HÖGSKOLAN

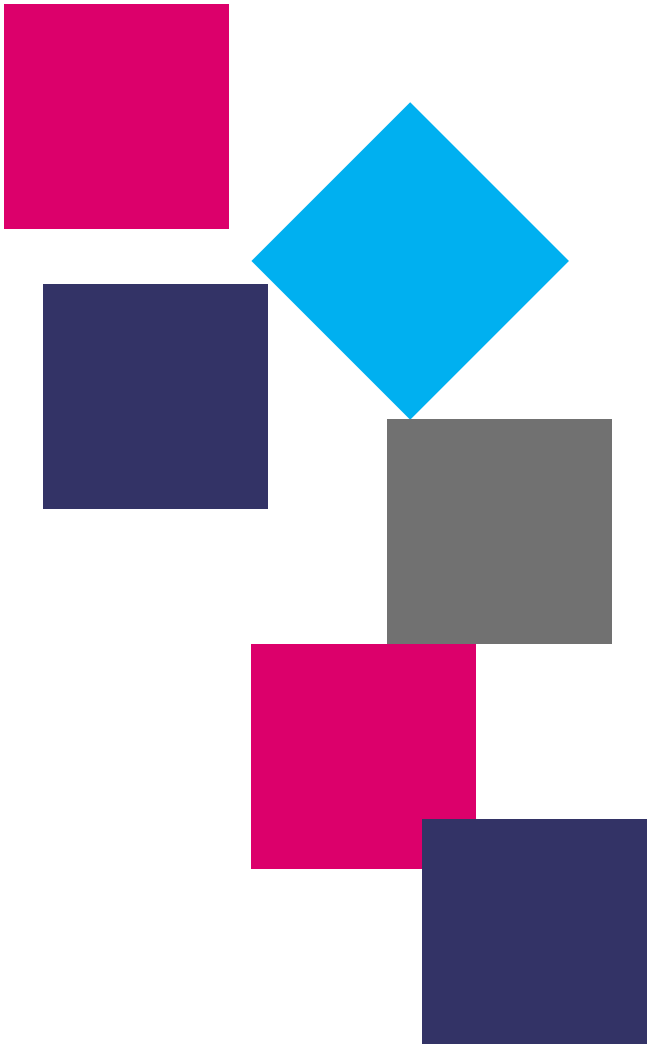
2013-12-17

European Aviation Crisis Management

CRISES CREST SOCIETY
ECONOMY TECHNOLOGY

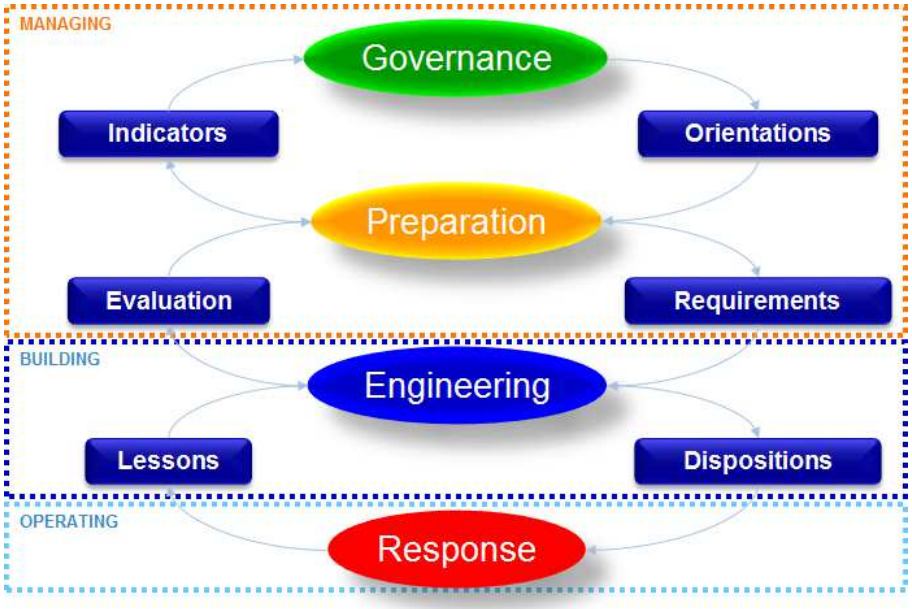
CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

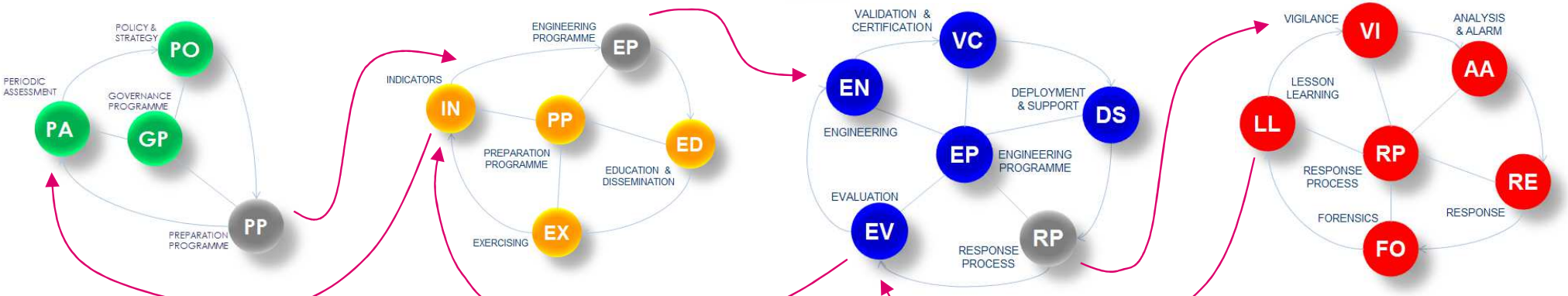
Governing resilience in the context of critical infrastructures



crest.researchgroup@gmail.com

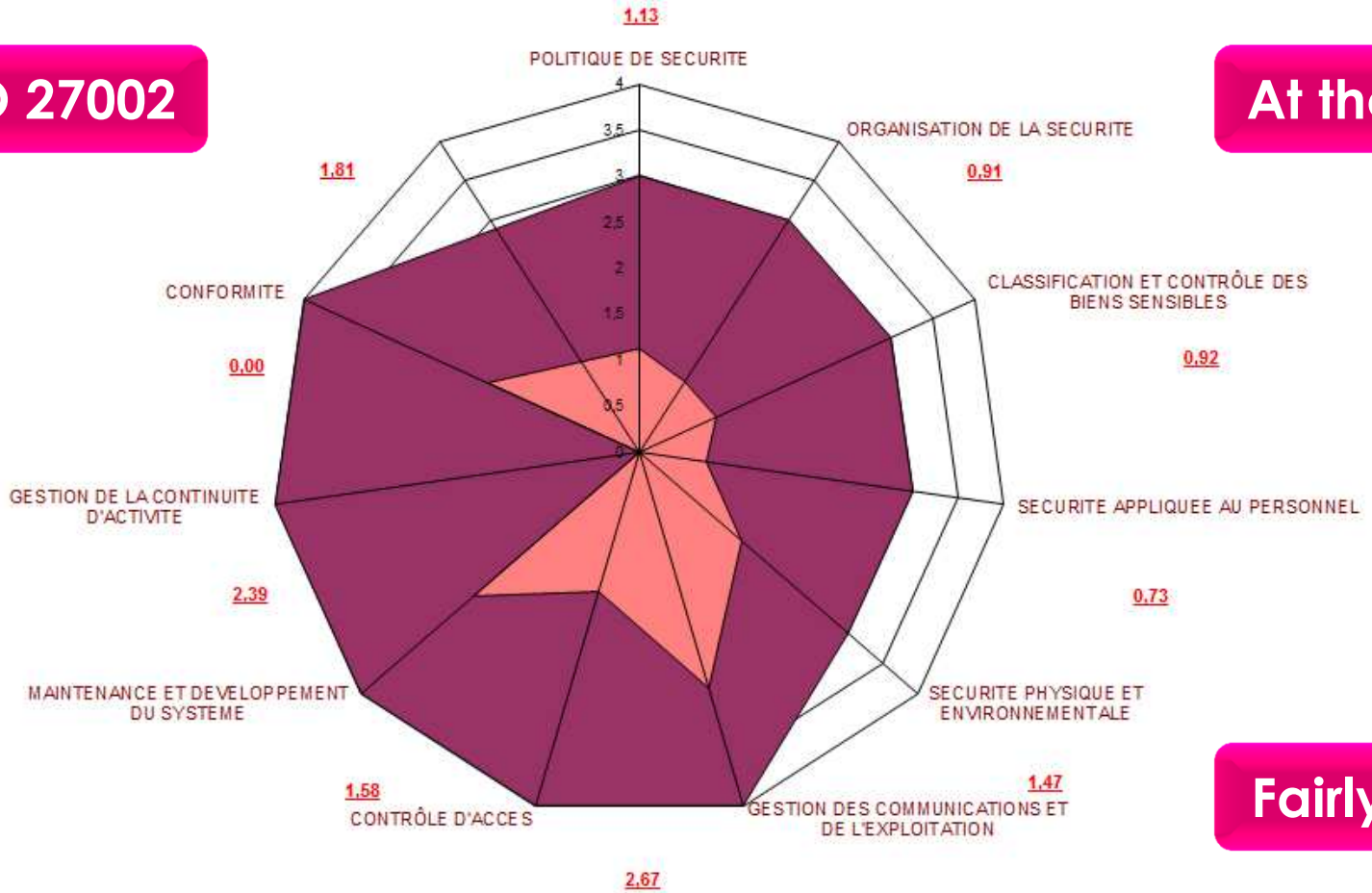
The general process of governance: levels, roles & activities





How is governance governed? Through standards such as…

ISO 27002



At the corporate level

Fairly flat, mono-level

But there are many more governance reference frameworks

FINANCE	US Security Exchange (Cybersecurity Roundtable 2014) http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt
NIST + Example of Energy	Federal Energy Regulatory Commission and North American Electric Reliability Corporation (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 And 2013 Cyber Security Standards Transition Guidance (Revised)
	NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity
	NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (SECURITY CONTROL BASELINES)
SPACE	Galileo programme (European Commission & European Space Agency)
TELECOMS	DG CNECT -ex DG INFSO- http://ec.europa.eu/ and ENISA
AVIATION / ATM	AIAA (2013). The Connectivity Challenge: Protecting Critical Assets in a Networked World. A Framework for Aviation Cybersecurity. Decision Paper, August 2013
	Eurocontrol (2012). Manual for National ATM Security Oversight
	ICAO (2011). Annex 17 to the Convention on International Civil Aviation. Security. 9th Edition, March 2011
	ICAO doc 8973 chapter 18 Cyber threats to critical aviation information and communication technology systems
	ICAO's AVIATION SECURITY PANEL (AVSECP) AVSECP - TWENTY-FOURTH MEETING Montréal, 8 to 12 April 2013
	AIAA
	NextGen
OTHER STANDARDS FOR CORPORATIONS	ISO 27002
	MITRE (2011) cyber resiliency engineering framework (Document MTR110237)
CIIP - Network & Information Security in Europe	ENISA. (2012). National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace.
	European Cyber Security Protection Alliance. (2014). D2.2.2 – Impact contribution and approaches – national policies and organisation. CYSPA, FP7-ICT-2011-8 / 318355.
	COM(2013) 48 Final : Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union

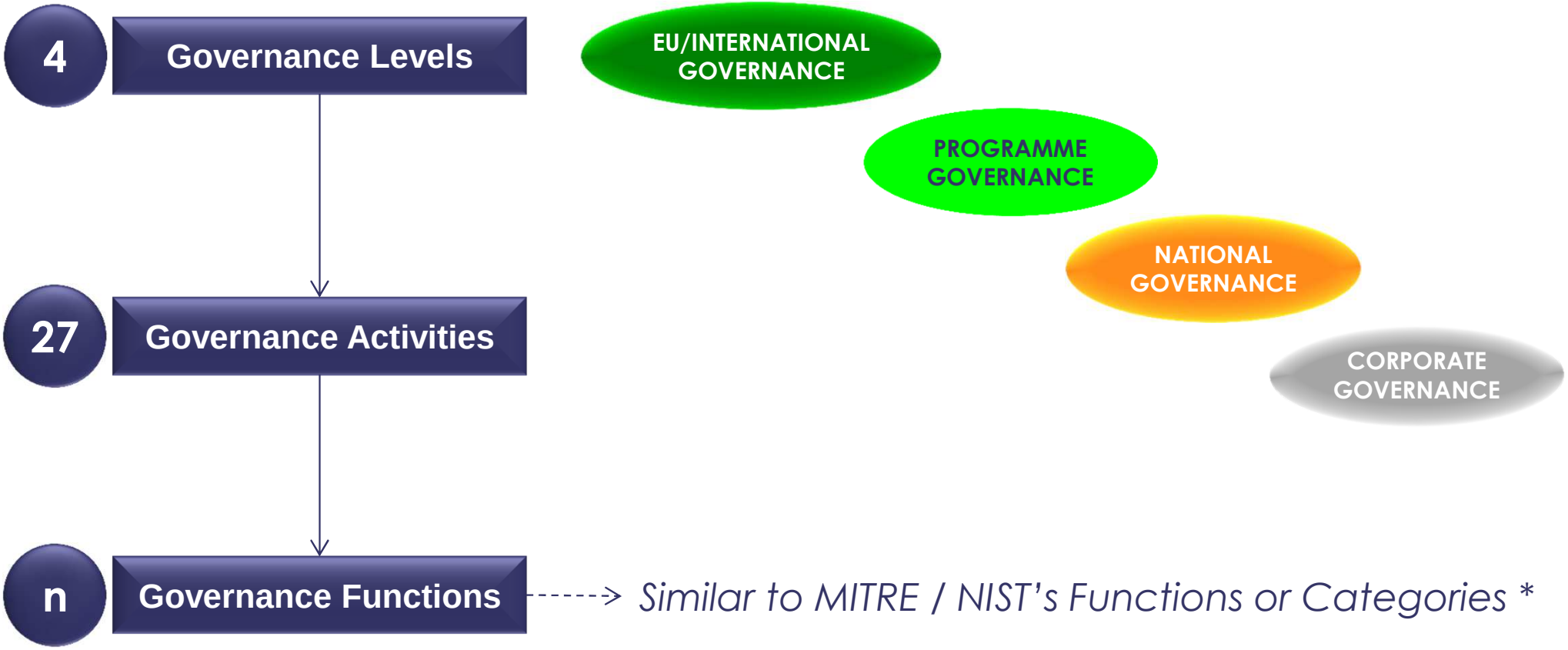
18 (2014)

+ legislation

+ NCSS *

* National Cyber Security Strategies

These 18 frameworks yield a list of governance activities…



*Similar to MITRE / NIST's Functions or Categories **

* MITRE (2011) cyber resiliency engineering framework. Document MTR110237.
NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity

… That form the multilevel governance framework

Policy, Regulation & Enforcement
Analysis & Dialog
Policy-making, Planning & Funding
R&D
Standardisation
Support & Awareness Raising
Common Cybersecurity Services

Legislation
Coordination & Collaboration

Governance programme
Preparation programme
Engineering programme
Response process

Legislation
Programme support

Today (mid 2016)

EU: the NIS Directive

- However, some exclusions following EP's resolution

EU: the CEN-CENELEC Cybersecurity Coordination Group (CSCG)

- On request from DG CONNECT
- Points to the need to coordinate cybersecurity standardisation across Europe

Sectorial initiatives

- Customisation of generic standards
- Creation of standards for EATM, Galileo, US Energy, etc.

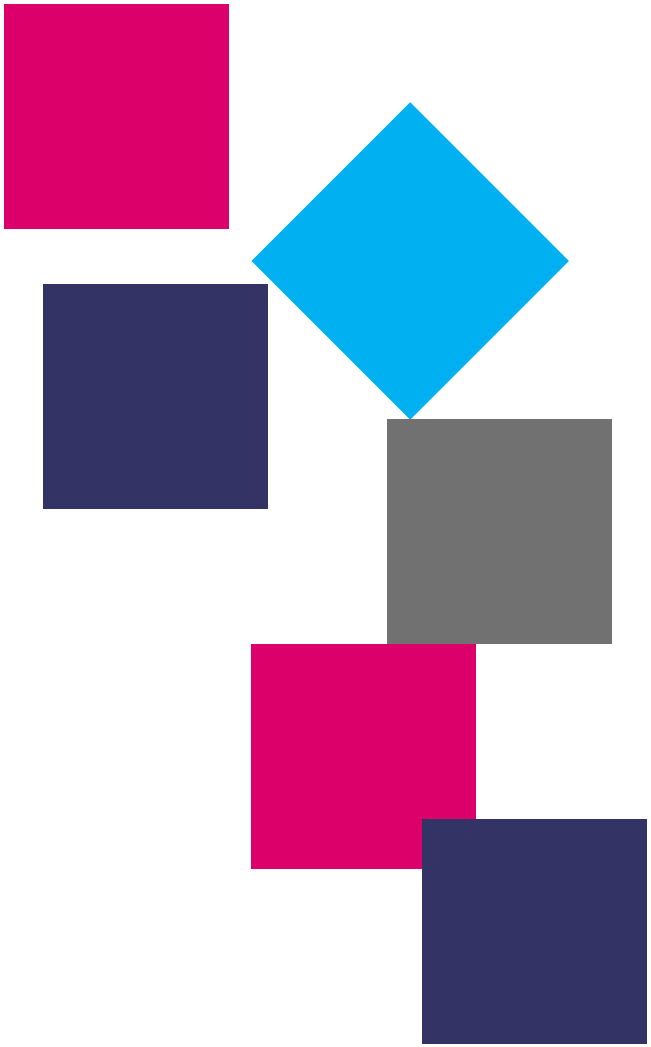
There is still work ahead

- But this shows an evolution of public policies

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

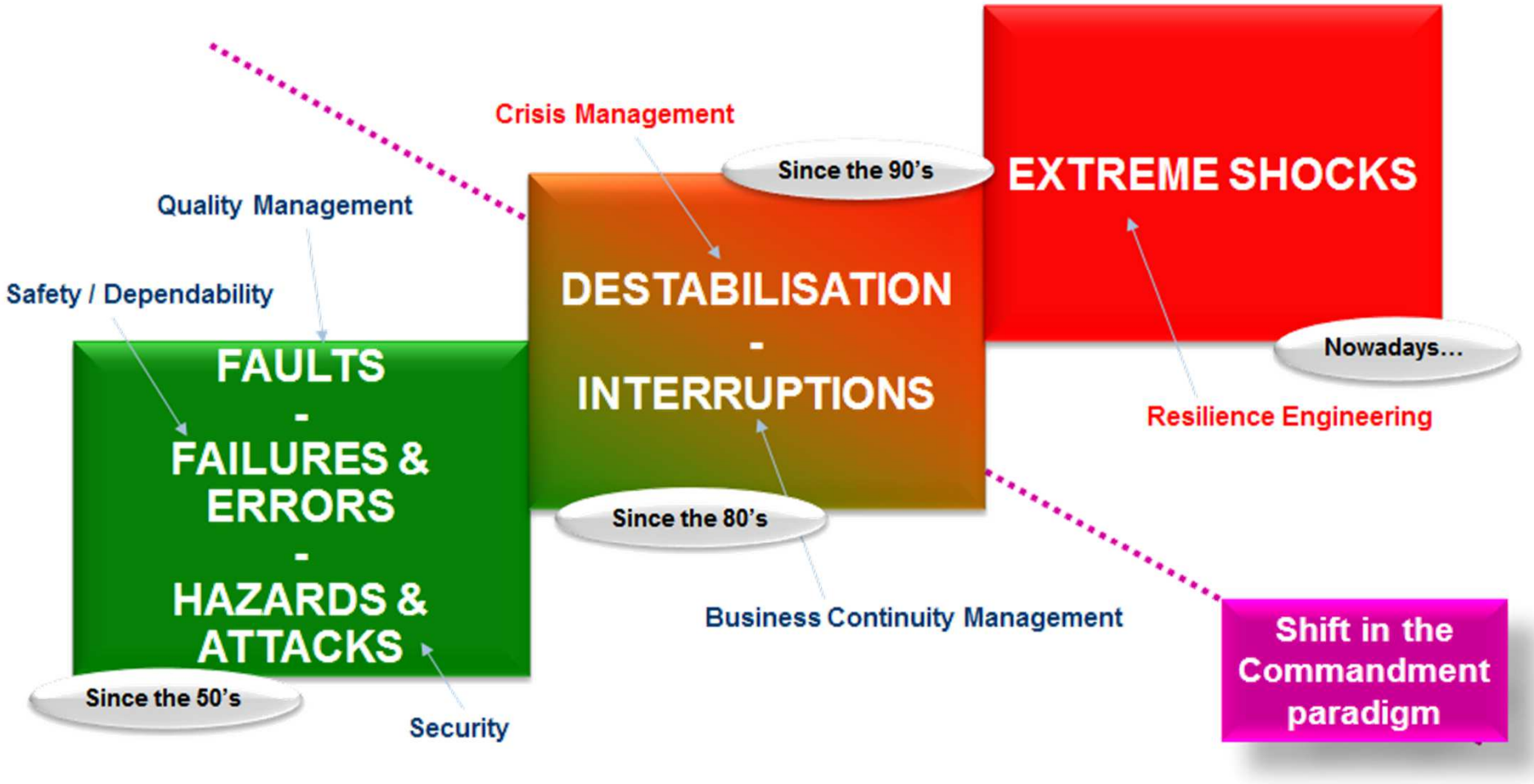
Conclusions

New standards for a doomed issue?



crest.researchgroup@gmail.com

Conclusion 1: The shift towards resilience has emerged…



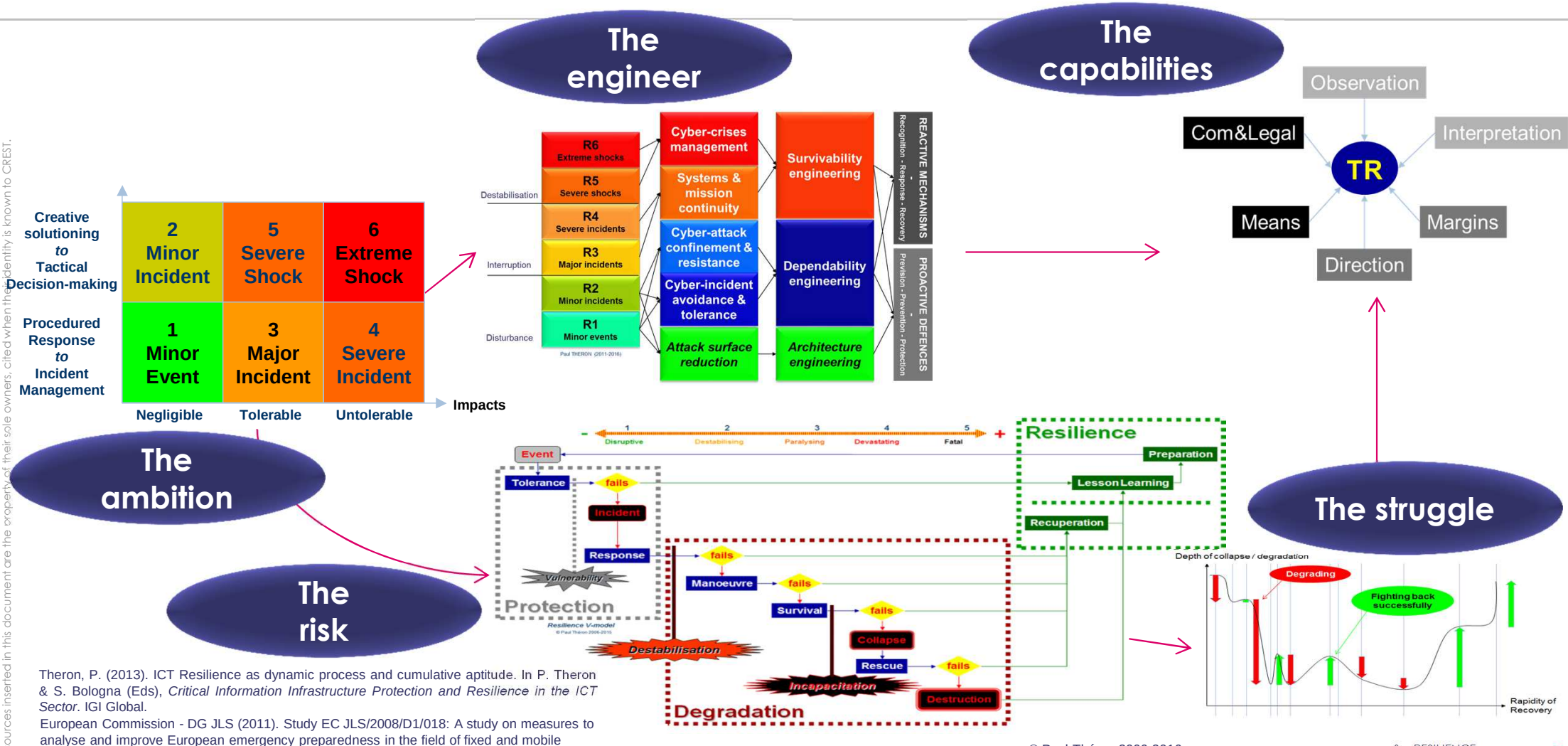
… from the recent concept of extreme shock

European Parliament (2011) Study Report on "*The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally*". Directorate General for Internal Policies ; Policy Department A: Economic and Scientific Policy ; Industry, Research and Energy, p21:

- *«A recent OECD study* analysed whether cyber-incidents could lead to a 'global shock' as devastating as e.g. large-scale pandemics.*
- *They concluded that there are a **very few cyber events with the capacity to provoke a global shock**.*
- *Although they state that there are many examples where cyber-incidents have caused a great deal of harm and financial loss, they conclude that the greatest concern for policy makers are large scale events caused by **two different cyber-incidents taking place at the same time or a cyber-event taking place during another form of disaster or attack**. »*

* OECD (2011) *Reducing Systemic Cybersecurity Risk*. P. Sommer, I. Brown, IFP/WKP/FGS(2011)

Conclusion 2: (Cyber) Resilience stems from empirical engineering



Theron, P. (2013). ICT Resilience as dynamic process and cumulative aptitude. In P. Theron & S. Bologna (Eds), *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. IGI Global.

European Commission - DG JLS (2011). Study EC JLS/2008/D1/018: A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet.
http://ec.europa.eu/information_society/policy/nis/strategy/prep_study/index_en.htm

Conclusion 3: Resilience engineering yields operational capabilities

Operational capabilities of resilient STS°

° Sociotechnical systems

P3R3 MECHANISMS	P3R3 OPERATIONAL CAPABILITIES
Prevision (of threats)	Cooperation between public & private agents
	Threat Intelligence (sources, means, …)
	Threat analysis (targets, vectors, potential, …)
	Evaluation of threat priorities
Prevention (of threats)	Reduction of threats at source or Deterrence
	Public authorities' support & Public-Private collaboration
Protection (of systems against residual threats)	Defence barriers engineering, deployment & operation
	Awareness Raising, Education & Training
	Management of systems' lifecycle & subcontractors
Recognition (of an incident)	Surveillance, Reconnaissance, & Detection of events
	Event analysis & Incident confirmation
	Alarm on incident
Response (to incidents in order to preserve missions & systems against residual risks)	Mobilisation process (confirmation, decision, activation)
	Commandment & operational chain & systems
	Reaction plans (defence, manœuvre, survival, rescue)
	Reaction (Forces & other tactical capacities)
	Traces management and exploitation & Forensics
	Investigations – Legal suits – Retaliation
Recovery (of missions & systems)	Lesson Learning & Sharing
	Repair & Reconstruction
	Adaptation & Improvement

… while related emerging concepts are now converging

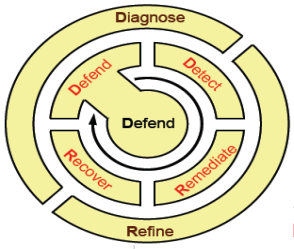
Mechanism	Goal	Activities
IDENTIFY	To develop the awareness of cyber-security risks to systems, assets, data, and capabilities.	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
PROTECT	To develop and implement safeguards appropriate to prevent adverse cybersecurity events that could harm the delivery of critical infrastructure services.	Access Control
		Awareness and Training
		Data Security
		Information Protection Processes and Procedures
		Maintenance
		Protective Technology
DETECT	To identify occurrences of cyber-security events and alarm ICT operators and business managers.	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
RESPOND	To develop and implement the activities appropriate to reacting to detected cybersecurity events	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
RECOVER	To develop and implement the activities appropriate to restore capabilities or services impaired by cybersecurity events and to improve cyber defence capabilities	Recovery Planning
		Improvements
		Communications

MITRE (2011) cyber resiliency engineering framework. Document MTR110237.

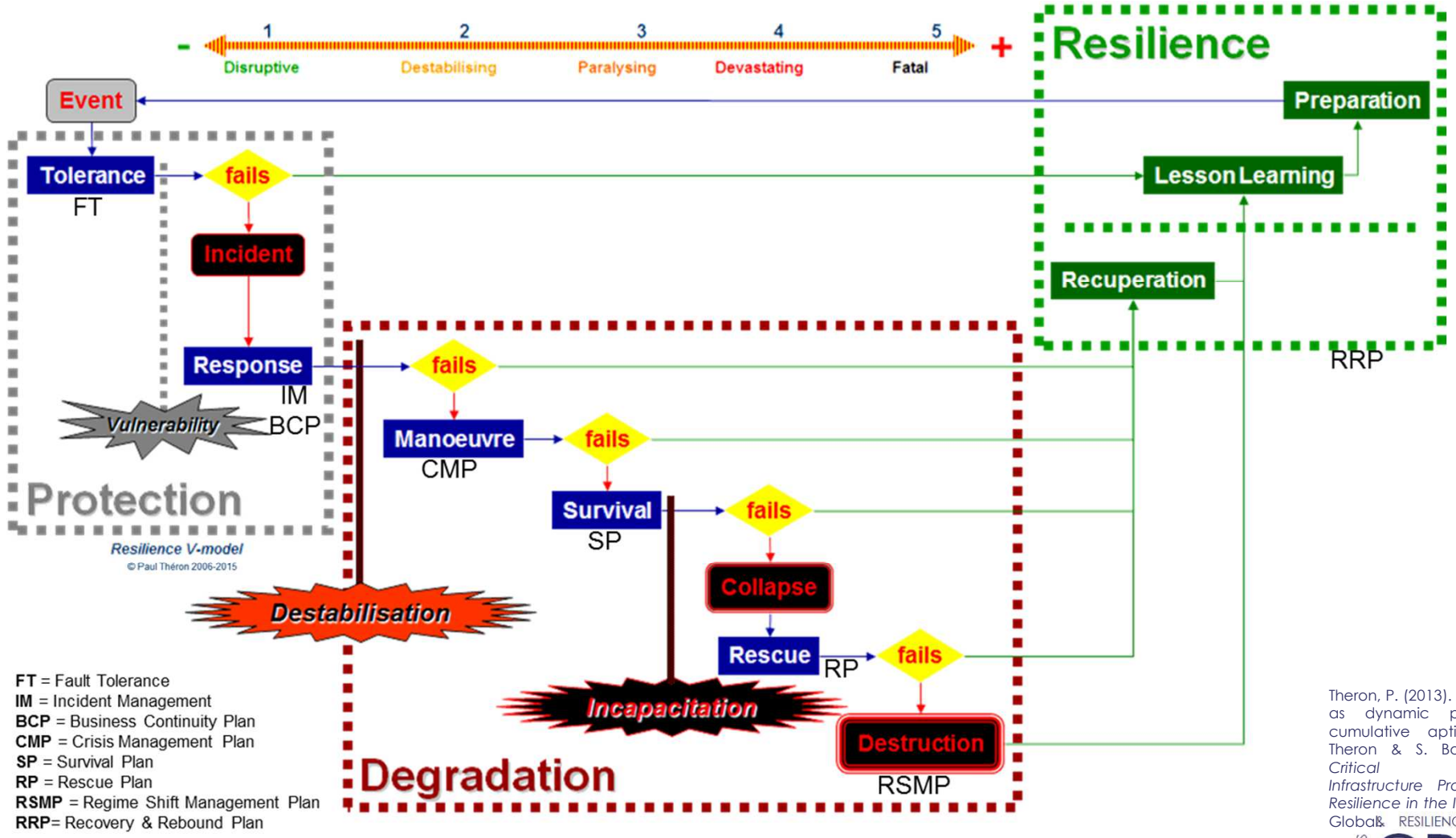
P3R3 MECHANISMS	P3R3 OPERATIONAL CAPABILITIES
Prevision (of threats)	Cooperation between public & private agents
	Threat Intelligence (sources, means, …)
	Threat analysis (targets, vectors, potential, …)
	Evaluation of threat priorities
Prevention (of threats)	Reduction of threats at source or Deterrence
	Public authorities' support & Public-Private collaboration
Protection (of systems against residual threats)	Defence barriers engineering, deployment & operation
	Awareness Raising, Education & Training
	Management of systems' lifecycle & subcontractors
Recognition (of an incident)	Surveillance, Reconnaissance, & Detection of events
	Event analysis & Incident confirmation
	Alarm on incident
Response (to incidents in order to preserve missions & systems against residual risks)	Mobilisation process (confirmation, decision, activation)
	Commandment & operational chain & systems
	Reaction plans (defence, manœuvre, survival, rescue)
	Reaction (Forces & other tactical capacities)
	Traces management and exploitation & Forensics
	Investigations – Legal suits – Retaliation
Recovery (of missions & systems)	Lesson Learning & Sharing
	Repair & Reconstruction
	Adaptation & Improvement

From Théron, P. (2013). ICT Resilience as Dynamic Process and Cumulative Aptitude. In P. Théron & S. Bologna (Eds.) *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 1-35. IGI Global, available at http://www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773.

Sterbenz J P G, Hutchinson D, Cetinkaya E C, Jabbar A, Rohrer J P, Schöller M & Smith P (2010). Resilience and survivability in communication networks: Strategies, principles and survey of disciplines. Preprint submitted to COMNET: Resilient and survivable networks, March 9th, 2010



Conclusion 4: Different levels of collapse require different plans…



Theron, P. (2013). ICT Resilience as dynamic process and cumulative aptitude. In P. Theron & S. Bologna (Eds), *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. IGI Global.

… which calls for a set of consistent resilience engineering standards

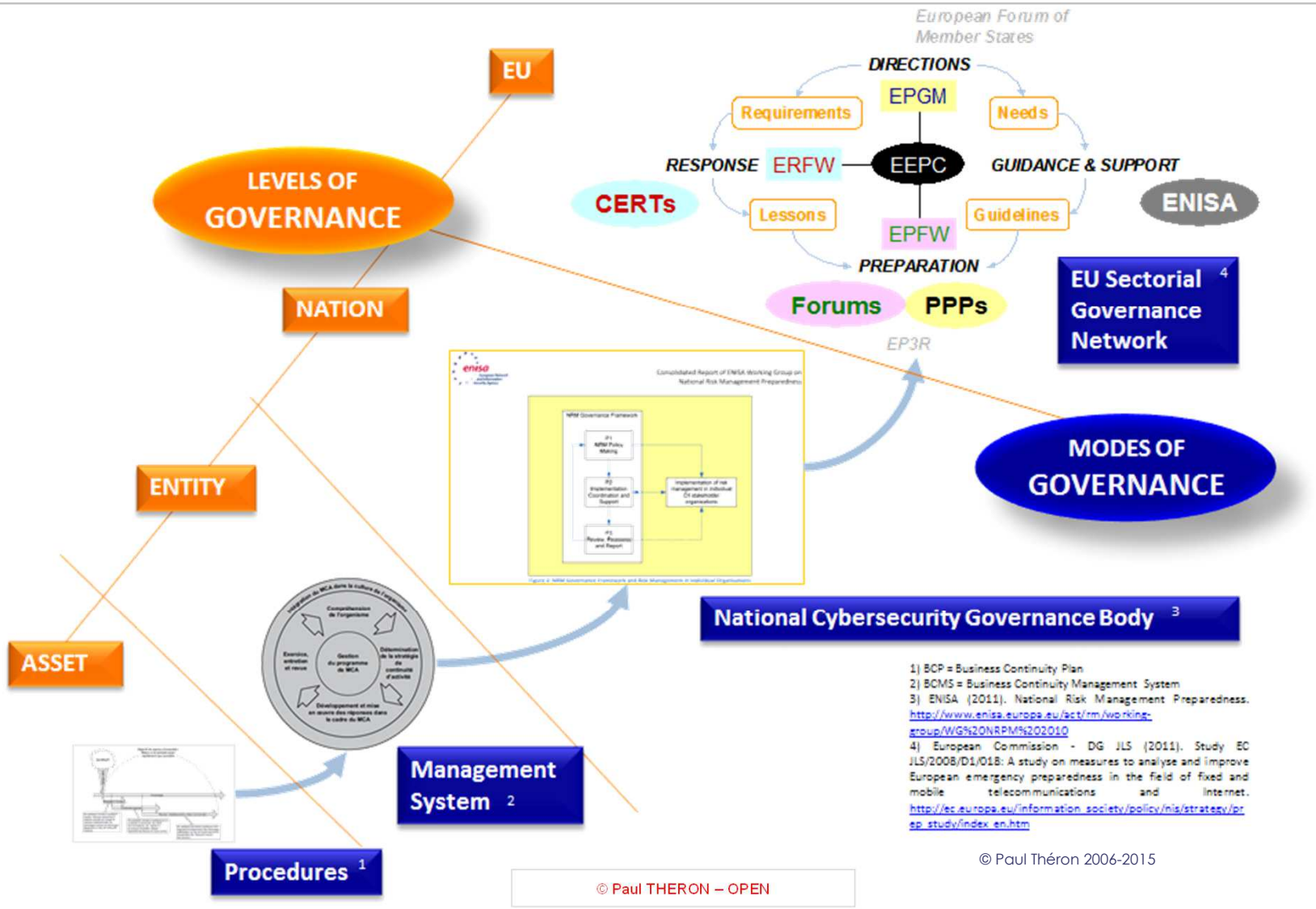
Further basic "technical" standards…

Collapse Ladder Levels	Required standards
1- Disruption (Planned response)	**Engineering, Incident Management, Business Continuity Management, …**
2- Destabilisation (Manoeuvre)	**Crisis Management**
3- Paralysis (Survival)	**Survival Management**
4- Devastation (Collapse & Rescue)	**Rescue Management**
5- Destruction (Fatal Regime shift)	**Regime Shift Management**

… plus a more global "multilevel governance" standard

Theron, P. (2013). ICT Resilience as dynamic process and cumulative aptitude. In P. Theron & S. Bologna (Eds), *Critical Information Infrastructure Protection and Resilience in the ICT Sector*. IGI Global.

Conclusion 5: Governing CIs' resilience is a multilevel challenge…

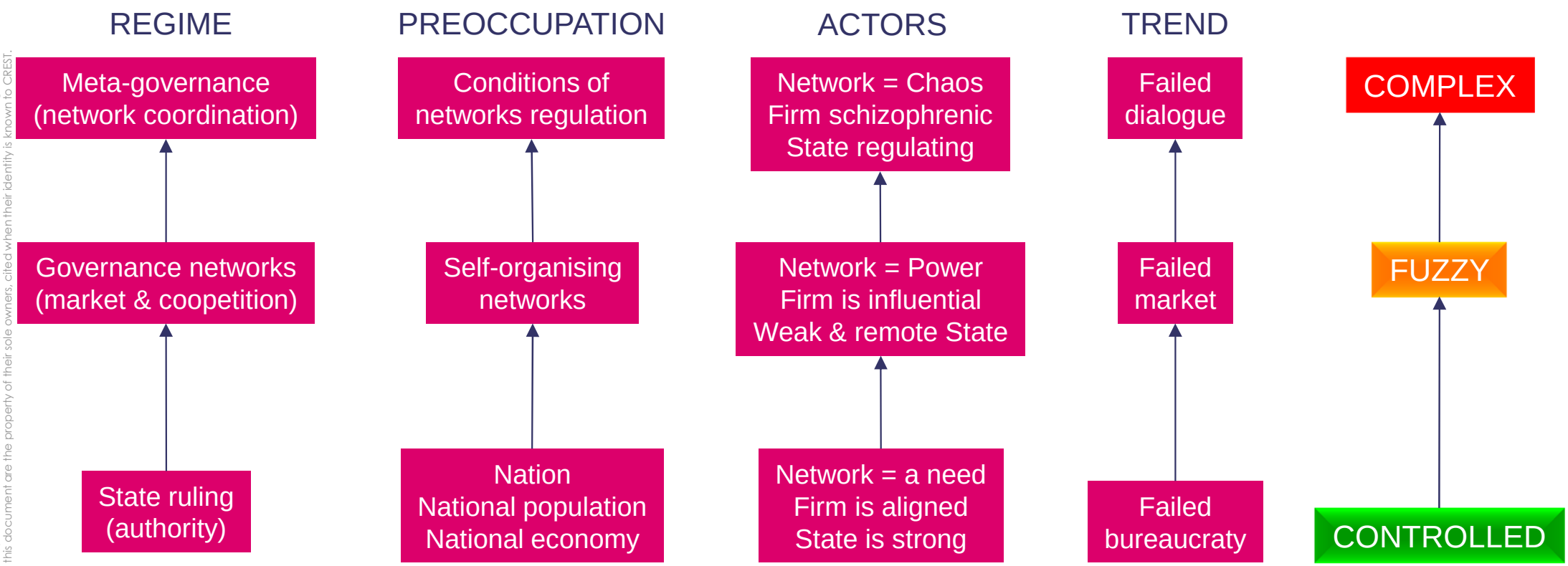


1) BCP = Business Continuity Plan
2) BCMS = Business Continuity Management System
3) ENISA (2011). National Risk Management Preparedness. http://www.enisa.europa.eu/act/rm/working-group/WG%20NRPM%202010
4) European Commission - DG JLS (2011). Study EC JLS/2008/D1/018: A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet. http://ec.europa.eu/information_society/policy/nis/strategy/prep_study/index_en.htm

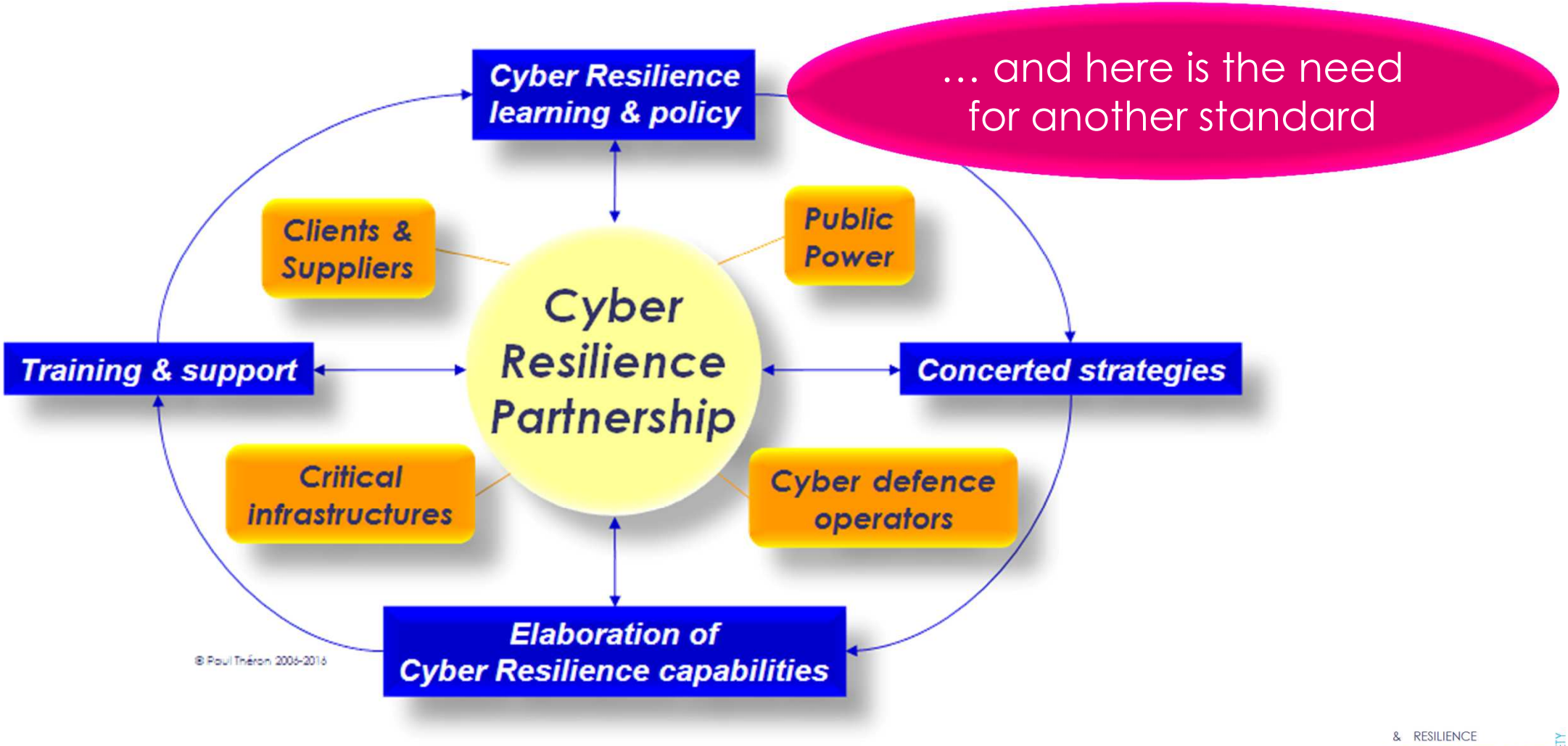
© Paul Théron 2006-2015

CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY

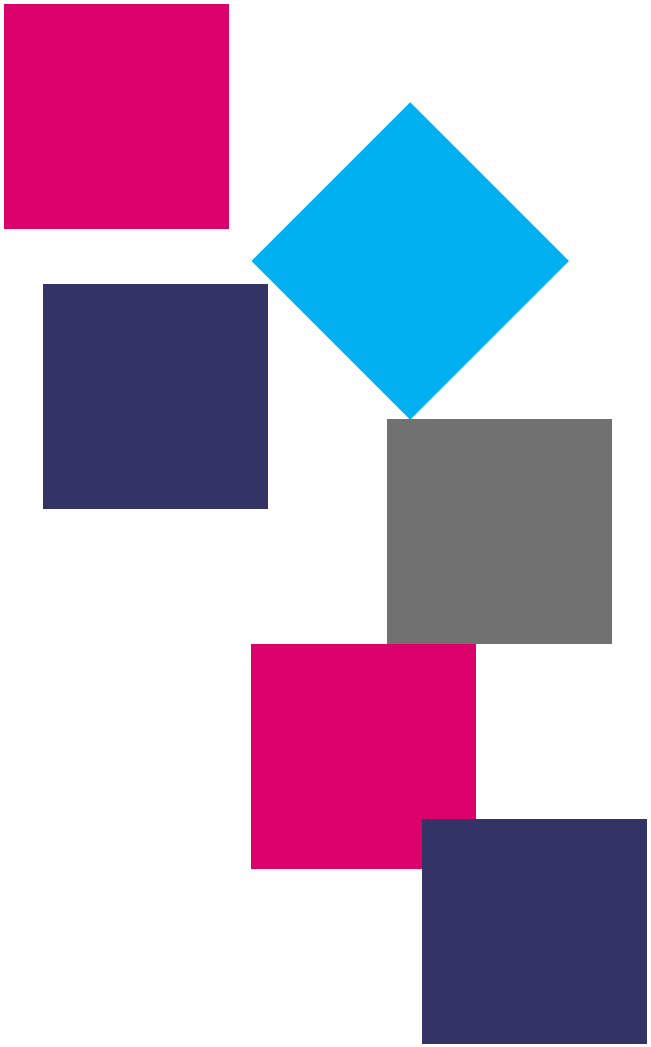
… in a difficult-to-control context of public management…



… which suggests short-term mitigation actions on the ground



CRISES & RESILIENCE CREST SOCIETY ECONOMY TECHNOLOGY



Thanks for your attention

Happy to answer your questions

crest.researchgroup@gmail.com

Some references online…

NIST website
ENISA website
OWASP website
MITRE website

Theron, P. (2009). Resilience, Incident Reporting and Exercises. Measuring Resilience – the Next Challenge. *ENISA Quarterly Review*, 5(4). Available at https://www.enisa.europa.eu/publications/eqr-archive/issues/eqr-q3-2009-vol.-5-no.-4.

European Commission - DG JLS (2011) *Study EC JLS/2008/D1/018: A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet*. Available at http://ec.europa.eu/information_society/policy/nis/strategy/prep_study/index_en.htm

ENISA (2011) Enabling and managing end-to-end resilience. Available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

ENISA (2011) *National Risk Management Preparedness*. Available at http://www.enisa.europa.eu/act/rm/working-group/WG%20NRPM%202010

Théron, P. (2011). Un nouveau paradigme pour l'étude des crises et de la résilience sociétale. *Cahiers de la sécurité*, 15, janvier-mars 2011, available at http://www.cahiersdelasecuriteetdelajustice.fr/content/cahiers-de-la-s%C3%A9curit%C3%A9-n%C2%B015.

Théron, P. (2011). *Seven Findings on Critical Infrastructures Resilience*. Lucern, Switzerland: CRITIS 2011 6th International Conference on Critical Information Infrastructures Security, September 8-9 2011, available at http://fr.slideshare.net/robbinlaird/critical-infrastructure-resilience.

Théron, P. (2011). *Three perspectives on Critical Infrastructure Resilience*. Brussels: ENISA/DG INFSO Workshop on resilience, 17/10/2011, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/metrics/ontology/presentations/theron.

Théron, P. (2013). ICT Resilience as Dynamic Process and Cumulative Aptitude. In P. Théron & S. Bologna (Eds.) *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 1-35. IGI Global, available at http://www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773.