
Paul Théron

To cite this version:


HAL Id: cel-01342846
https://halshs.archives-ouvertes.fr/cel-01342846v2
Submitted on 17 Jul 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

ERNCIP lecture, Brussels, 22/06/2016
Paul THERON, PhD, FBCI
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/cognitionresilience/traitrauma/home
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
What is resilience?
Case studies all point to a common phenomenon...

Resilience is a struggle against collapse
Collapse in New-Orleans (Katrina, August 2005)

Preparing for the expected

- Alarm
- Evacuation
- Refuge
- Last precautions

Fighting unexpectedness

- After-shock
- Security restauration
- Déploiement
- Incidents
- Preparation of rescue
- Survival
- Shock
- Devastation

© Paul THERON – OPEN

Collapse in New-Orleans (Katrina, August 2005)
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)

Fire is 100/200 yards away

**Disruption**

**Planned response**
Dodge orders to run south up the canyon
Dodge orders to drop tools
Dodge invents escape fire
Sallee and Rumsey take refuge in a crevice

**Tactics**
fails

**Destabilising circumstances**

**Fire catches up on men**

**Overwhelming circumstances**

**Survival**
fails

**Collapse**

**Rescue**
fails

**Destruction**
12 smokejumpers have perished altogether

Fire about to explode into a fire whirl
Fire explodes into a fire whirl

Some smokejumpers seriously wounded
Wounds too serious

Dodge, Sallee and Rumsey finally safe

**Recovery**
Lieutenant A & the rottweilers: a cognitive struggle for safety

Fighting for self-preservation

http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.616373
Recent techno-focused literature too…

Resilience is confirmed to be a struggle against collapse
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)
- 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

This page contains a diagram illustrating the phases of a resilient response to an incident. The diagram shows the following phases:

- Event
- Detection
- Immediate Response
- Service Recovered
- Capacity for Resilience
- Repair and/or Replacement
- System Restored
- Degradation
- Time

The diagram highlights the timeline and service level during the various stages of an incident, from initial impact to recovery and system restoration.
Survivability (Sterbenz & al., 2010)

Figure 6: Resilience State Space

© Paul THERON – OPEN
A definition of resilience

7 findings & precepts about resilience
1st finding: why it is needed (Accept that complexity will defeat you)

Complexity stemming from interdependencies

Complexity of a crisis-prone society
2nd finding: why it is so misunderstood (Think beyond words)

Fragile

Robust

Resilient

pressure

more pressure

more pressure

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

**Prevention**
- Anticipating threats
  - **Prevision**
  - **Restoration**
    - Restoring nominal capabilities
  - **Response**
    - Seeking tactical control of CoT *
  - **Protection**
    - Defending sociotechnical systems
  - **Recognition**
    - Identifying incidents

**THREAT**
- Non-reducible threat
- Residual damage
- Residual threat

**P3R3**
- Anticipating threats
- Reducing threat at source
- Defending sociotechnical systems
- Identifying incidents
- Restoring nominal capabilities
- Seeking tactical control of CoT *

**AVOIDING**
- Prevision
- Prevention
- Protection
- Response
- Restoration

**COPING**
- Recognition
- Residual damage

**INCIDENT**

* Course of Things
7th finding: how it is governed (Prepare to collaborate)
Governing resilience in the context of critical infrastructures
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

<table>
<thead>
<tr>
<th>Section</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>FINANCE</td>
<td>US Security Exchange (Cybersecurity Roundtable 2014)</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.see.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt">http://www.see.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt</a></td>
</tr>
<tr>
<td>NIST + Example of Energy</td>
<td>Federal Energy Regulatory Commission and North American Electric Reliability Corporation</td>
</tr>
<tr>
<td></td>
<td>(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1</td>
</tr>
<tr>
<td></td>
<td>And 2014 Cyber Security Standards Transition Guidance (Revised)</td>
</tr>
<tr>
<td></td>
<td>NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity</td>
</tr>
<tr>
<td></td>
<td>NIST Special Publication 800-63 Revision 4</td>
</tr>
<tr>
<td></td>
<td>Security and Privacy Controls for Federal Information Systems and Organizations (SECURITY CONTROL BASELINES)</td>
</tr>
<tr>
<td>SPACE</td>
<td>Galileo programme</td>
</tr>
<tr>
<td></td>
<td>ICAO doc 89F3 chapter 18</td>
</tr>
<tr>
<td></td>
<td>Cyber threats to critical aviation information and communication technology systems</td>
</tr>
<tr>
<td></td>
<td>ICAO’s AVIATION SECURITY PAREL (AVSECP)</td>
</tr>
<tr>
<td></td>
<td>AVSECP - TWENTY-FOURTH MEETING Montreal, 8 to 12 April 2013</td>
</tr>
<tr>
<td></td>
<td>AIAA</td>
</tr>
<tr>
<td></td>
<td>NextGen</td>
</tr>
<tr>
<td></td>
<td>ISO 27002</td>
</tr>
<tr>
<td>AVIATION / ATM</td>
<td></td>
</tr>
<tr>
<td>OTHER STANDARDS FOR CORPORATIONS</td>
<td>MITRE (2011) cyber resiliency engineering framework (Document MTR116237)</td>
</tr>
</tbody>
</table>

* National Cyber Security Strategies
These 18 frameworks yield a list of governance activities…

4. Governance Levels

- EU/INTERNATIONAL GOVERNANCE
- PROGRAMME GOVERNANCE
- NATIONAL GOVERNANCE
- CORPORATE GOVERNANCE

27. Governance Activities

n. Governance Functions

Similar to MITRE / NIST’s Functions or Categories *

NIST (2014) Framework for Improving Critical Infrastructure Cybersecurity
... That form the multilevel governance framework
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
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. »

Conclusion 2: (Cyber) Resilience stems from empirical engineering


© Paul Théron 2006-2016
Conclusion 3: Resilience engineering yields operational capabilities

Operational capabilities of resilient STS°

° Sociotechnical systems

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

© Paul THERON – OPEN
... while related emerging concepts are now converging

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


Table: P3R3 OPERATIONAL CAPABILITIES

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>P3R3 OPERATIONAL CAPABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention</td>
<td>Cooperation between public &amp; private agents</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Source, means, ...</td>
</tr>
<tr>
<td>Threat Analysis</td>
<td>Targets, vectors, potential, ...</td>
</tr>
<tr>
<td>Evaluation of Threat Priorities</td>
<td></td>
</tr>
<tr>
<td>Public Authorities' Support</td>
<td>&amp; Public-Private collaboration</td>
</tr>
<tr>
<td>Protection</td>
<td>Defence barriers engineering, deployment &amp; operation</td>
</tr>
<tr>
<td>Awareness Raising Education &amp; Training</td>
<td></td>
</tr>
<tr>
<td>Management of systems' lifecycle &amp; subcontractors</td>
<td></td>
</tr>
<tr>
<td>Recognition</td>
<td>Surveillance, Reconnaissance, &amp; Detection of events</td>
</tr>
<tr>
<td>Event Analysis &amp; Incident Confirmation</td>
<td></td>
</tr>
<tr>
<td>Alarm on incident</td>
<td></td>
</tr>
<tr>
<td>Response</td>
<td>Mobilisation process (confirmation, decision, activation)</td>
</tr>
<tr>
<td>Command &amp; operational chain &amp; systems</td>
<td></td>
</tr>
<tr>
<td>Reaction plans (defence, manoeuvre, survival, rescue)</td>
<td></td>
</tr>
<tr>
<td>Reaction (forces &amp; other tactical capacities)</td>
<td></td>
</tr>
<tr>
<td>Traces management and exploitation &amp; Forensics</td>
<td></td>
</tr>
<tr>
<td>Investigations – Legal suits – Retaliation</td>
<td></td>
</tr>
<tr>
<td>Recovery</td>
<td>Lesson Learning &amp; Sharing</td>
</tr>
<tr>
<td>Repair &amp; Reconstruction</td>
<td></td>
</tr>
<tr>
<td>Adaptation &amp; Improvement</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion 4: Different levels of collapse require different plans…

FT = Fault Tolerance
IM = Incident Management
BCP = Business Continuity Plan
CMP = Crisis Management Plan
SP = Survival Plan
RP = Rescue Plan
RSMP = Regime Shift Management Plan
RRP = Recovery & Rebound Plan

© Paul THERON – OPEN
... which calls for a set of consistent resilience engineering standards

<table>
<thead>
<tr>
<th>Collapse Ladder Levels</th>
<th>Required standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1- Disruption (Planned response)</td>
<td>Engineering, Incident Management, Business Continuity Management, …</td>
</tr>
<tr>
<td>2- Destabilisation (Manoeuvre)</td>
<td>Crisis Management</td>
</tr>
<tr>
<td>3- Paralysis (Survival)</td>
<td>Survival Management</td>
</tr>
<tr>
<td>4- Devastation (Collapse &amp; Rescue)</td>
<td>Rescue Management</td>
</tr>
<tr>
<td>5- Destruction (Fatal Regime shift)</td>
<td>Regime Shift Management</td>
</tr>
</tbody>
</table>

Further basic “technical” standards...

... plus a more global “multilevel governance” standard

Conclusion 5: Governing CIs’ resilience is a multilevel challenge...
... in a difficult-to-control context of public management...

**REGIME**
- Meta-governance (network coordination)
- Governance networks (market & coopetition)
  - State ruling (authority)

**PREOCCUPATION**
- Conditions of networks regulation
- Self-organising networks
  - Nation
    - National population
    - National economy

**ACTORS**
- Network = Chaos
  - Firm is schizophrenic
    - Weak & remote State
- Network = Power
  - Firm is influential
    - Weak & remote State
- Network = a need
  - Firm is aligned
    - State is strong

**TREND**
- Failed dialogue
- Failed market
- Failed bureaucracy

**COMPLEX**
**FUZZY**
**CONTROLLED**
... which suggests short-term mitigation actions on the ground

... and here is the need for another standard
Thanks for your attention

Happy to answer your questions
Some references online…

NIST website
ENISA website
OWASP website
MITRE website


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%A9cur%C3%A9-et-de-la-justice/15/jan-mars-2011/un-nouveau-paradigme-pour-l%27%C3%A9tude-des-crises-et-de-la%C3%A9l%C3%A9ance-soci%C3%A9tale.

