Resilience is the Operational Branch of Sustainability: Intergenerational Equity

Contracting for Resilient Space Infrastructures

2017 Manfred Lachs, IASL, McGill

Mrs Maria LUCAS-RHIMBASSEN
Under the supervision of Professor Lucien RAPP

© 2017 Chaire SIRIUS – University Toulouse 1 Capitole
ORGAN RECITALS SERIES

ORGAN AND SPACE: GAZE UP TO THE HEAVENS
MAISON SYMPHONIQUE DE MONTRÉAL

The grand pianocent takes "Our Celestes" take place one hour before the concert.

Since the dawn of time, humans have turned their gaze towards the heavens. Uncovering the universe around them, from what is out of sight, allowed them to learn more about the planet they call home. Astronaut Lucile Saint-Jacques discussed this perpetual search for knowledge in a recital featuring music by Karl, Glass, Cappuccio and Dufourny, as well as a new work by Matthew Ricketts. Reflections and music come together against a backdrop of images of space and the Earth provided by the International Space Station.

TICKETS PRICES
From 43$*

SATURDAY MAY 6 2017 2:30 PM

ARTISTS AND PROGRAM | PRESENTATION OF THE CONCERT

SUBSCRIBE NOW
1-888-842-9951

MONTHS:

MAY, 2017

1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
BUT NOW, MILITARY APPROACH

- Contested, congested, competitive.
- "Resiliency is the ability of a system architecture to continue providing required capabilities in the face of system failures, environmental challenges, or adversary actions."


**RESILIENCE**

<table>
<thead>
<tr>
<th>DISAGGREGATION</th>
<th>DISTRIBUTION</th>
<th>DIVERSIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTECTION</td>
<td>PROLIFERATION</td>
<td>DECEPTION</td>
</tr>
</tbody>
</table>

## 2. UNDERSTANDING RISKS


### SPACE INFRASTRUCTURE

<table>
<thead>
<tr>
<th>TARGET</th>
<th>NON-INTENTIONAL</th>
<th>INTENTIONAL</th>
<th>EFFECT</th>
<th>MITIGATION MEASURES</th>
<th>PRIORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>space debris</td>
<td>physical damage</td>
<td></td>
<td></td>
<td>TCBMs, hardening, shielding, SST</td>
<td>high</td>
</tr>
<tr>
<td>space weather</td>
<td>bugs, damage</td>
<td></td>
<td></td>
<td>SSA, software, monitoring</td>
<td>high</td>
</tr>
<tr>
<td>unknown space phenomena</td>
<td>failure</td>
<td></td>
<td></td>
<td>redundancy, hardening, resilience, R&amp;D</td>
<td>medium</td>
</tr>
<tr>
<td>KEW/ASAT</td>
<td>partial/total destruction</td>
<td></td>
<td></td>
<td>international law, ITAR, rules, TCBMs, deterrence</td>
<td>very low</td>
</tr>
<tr>
<td>EMP (h alt nuc.)</td>
<td>destruction, Van Allen</td>
<td></td>
<td></td>
<td>international law, ITAR, rules, TCBMs, deterrence</td>
<td>low</td>
</tr>
<tr>
<td>DEW (energy)</td>
<td>signal disturbance, mechanical destruction</td>
<td></td>
<td></td>
<td>various</td>
<td>medium</td>
</tr>
<tr>
<td>laser-based ASAT</td>
<td>sensors/mechanical damage</td>
<td></td>
<td></td>
<td>classified</td>
<td>high</td>
</tr>
<tr>
<td>HPM ASAT (microwave)</td>
<td>sensors blinded, receivers and elec. degl.</td>
<td></td>
<td></td>
<td>self-protecting devices</td>
<td>medium</td>
</tr>
<tr>
<td>EW (E-war)</td>
<td>signal loss, satellite control loss</td>
<td></td>
<td></td>
<td>various</td>
<td>very high</td>
</tr>
<tr>
<td>jammers</td>
<td>radarsat/satcom incapacitation</td>
<td></td>
<td></td>
<td>waveforms, nulling antennas, beamforming, jam</td>
<td>very high</td>
</tr>
<tr>
<td>cyber attacks</td>
<td>transponder hijack, sat degr. info loss,</td>
<td></td>
<td></td>
<td>cryptography, secured software, process standard</td>
<td>very high</td>
</tr>
<tr>
<td>natural disaster</td>
<td>loss of comm w/ set, ground segm disrupt</td>
<td></td>
<td></td>
<td>redundancy, hardening, physical security measures</td>
<td>medium</td>
</tr>
<tr>
<td>ground infrastructure</td>
<td>loss of comm w/ set, ground segment</td>
<td></td>
<td></td>
<td>redundancy, hardening, physical security measures</td>
<td>medium</td>
</tr>
<tr>
<td>sabotage</td>
<td>loss of comm w/ set, ground segment</td>
<td></td>
<td></td>
<td>hardening</td>
<td>medium</td>
</tr>
<tr>
<td>cyber attacks</td>
<td>denial of service, info stolen/compromised</td>
<td></td>
<td></td>
<td>cryptography, authorit. proc. integrity checks</td>
<td>very high</td>
</tr>
<tr>
<td>data links</td>
<td>info compromised</td>
<td></td>
<td></td>
<td>radio-f o ord at national/international, null ant., wfm</td>
<td>high</td>
</tr>
<tr>
<td>interference</td>
<td>denial of service/comms/radar systems</td>
<td></td>
<td></td>
<td>radio-f o ord at national/international, null ant., wfm</td>
<td>medium</td>
</tr>
<tr>
<td>spoofing</td>
<td>wrong informatic proved</td>
<td></td>
<td></td>
<td>cryptography, authentif. proc. integrity checks</td>
<td>medium</td>
</tr>
<tr>
<td>cyber attacks</td>
<td>denial of service</td>
<td></td>
<td></td>
<td>cryptography, secure d software</td>
<td>very high</td>
</tr>
<tr>
<td>interception</td>
<td>information compromised</td>
<td></td>
<td></td>
<td>cryptography, specific waveforms</td>
<td>high</td>
</tr>
</tbody>
</table>

### TECHNOLOGY/INDUSTRY

<table>
<thead>
<tr>
<th>TARGET</th>
<th>NON-INTENTIONAL</th>
<th>INTENTIONAL</th>
<th>EFFECT</th>
<th>MITIGATION MEASURES</th>
<th>PRIORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>tech transfer</td>
<td>3rd party space progr competition for</td>
<td></td>
<td></td>
<td>coordinate export control, space industrial policy</td>
<td>high</td>
</tr>
<tr>
<td>supply shortage</td>
<td>no system deployed</td>
<td></td>
<td></td>
<td>space industrial policy</td>
<td>high</td>
</tr>
<tr>
<td>lack of launch opportunities</td>
<td>satellite grounded</td>
<td></td>
<td></td>
<td>european launch policy, framework contracts</td>
<td>medium</td>
</tr>
<tr>
<td>loss of industry know-how</td>
<td>no system deployed</td>
<td></td>
<td></td>
<td>space industrial policy, space R&amp;D programmes</td>
<td>medium</td>
</tr>
<tr>
<td>loss of spectrum and orbital resources</td>
<td>no system deployed</td>
<td></td>
<td></td>
<td>coordinated Exposition at European and ITU levels</td>
<td>high</td>
</tr>
<tr>
<td>new/ Firmware, supply chain under stress</td>
<td>hack</td>
<td></td>
<td></td>
<td>industrial policy</td>
<td>high</td>
</tr>
</tbody>
</table>

### SOLUTIONS

- TCBMs, hardening, shielding, SST
- SSA, software, monitoring
- Redundancy, hardening, resilience, R&D
- International law, ITAR, rules, TCBMs, deterrence
- Various
- Classified
- Self-protecting devices
- Various
- Waveforms, nulling antennas, beamforming, jam
- Cryptography, secured software, process standard
- Redundancy, hardening, physical security measures
- Redundancy, hardening, physical security measures
- Hardening
- Cryptography, authentic. proc. integrity checks
- Radio-f o ord at national/international, null ant., wfm
- Cryptography, authentic. proc. integrity checks
- Cryptography, secure d software
- Cryptography, specific waveforms

1. CRITICAL SPACE INFRASTRUCTURES (CSI)

- CSIs/CIs **interdependencies**. We can no longer isolate CIs in silos. **INTERCONNECTEDNESS**
- Space systems (circa 1300) on the rise, dual distinction blurred.

<table>
<thead>
<tr>
<th>ICS/IC</th>
<th>Energy</th>
<th>ICT</th>
<th>Water</th>
<th>Food</th>
<th>Health</th>
<th>Finance</th>
<th>Defense, National Security</th>
<th>Administration</th>
<th>Transport</th>
<th>Chemical and Nuclear Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Sensing</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Communication</td>
<td>2</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Meteorology</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>GNSS</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>Nanosatellites</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Space stations</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Rockets</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Space Probes</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

1. The infrastructures are related but the interaction is of little importance
2. The interaction is important but only for a few of the CI components, leading to a diffuse and indirect dependence towards the SCI
3. The infrastructures interact strongly and in some cases it can be said that there is a degree of direct dependence of the CI on the SCI
4. The dependence of CI on SCI is important but does not represent a threat
5. CI is fully dependent on the SCI activity and its perturbation would cause a potential irremediable deterioration and a disruption of CI functions
6. Both infrastructures strongly interact and are dependent on each other, the disruption of one causing the disruption of the other

Source: 4th IAA conference on CSI

*Figure 2: CI – SCI interaction (interaction from CRITSYS)*
INTERDEPENDENT VULNERABILITY

- CSI risks and sources of threat expand to other CIs. Transboundary, cross-sectoral issue.

- USA recognized CSI. In Europe: problem of governance, conflicting priorities.

- Sources of threat: cross-sectoral, transboundary and beyond.

- Categories: 1) Non-intentional/natural, 2) intentional, 3) technology/industry
  - Hardware (operational, kinetic), software (cyber), firmware (in-built, structural, supply chain)

- Targets: Space/Ground infrastructures and Data-links.

• Mitigating measures: international law, TCBMs, hardening, cryptography, export control, SST/SSA, monitoring, resilience, radio-frequency coordination, redundancy, industrial policy (procurement proposals), secure cloud, etc.

- SOLUTIONS: LAW? REGULATION? PATENTS? CONTRACTS?

SPACE... more than GPS, GNSS and SATCOM. Need to broaden to space assets
5. ALTERNATIVE: CONTRACTS.

SPACE IS A RISKY BUSINESS …

BUT WE HAVE SPACE LAW!

• Space = privatization transition.

• Space contracts = combination of existing clauses in a specific context (high tech, high risk)

• E.g: satellite purchase, supply of services manufacturing, operations, launching services, leasing of transponders, sale of imagery.

• Incentives = debate whether taken for granted. Penalties?

• Cross-waivers = hypothesis that they increase the level of resilience.

• Best efforts = enough? A model for resilience?

• Alternate and back up agreements (Mitsubishi, GNSS, Paradigm, transponders).

• Force majeure = need to change in order to incorporate risk. “Space is hard”
## Clauses Closest to Service Assurance

<table>
<thead>
<tr>
<th>Clause</th>
<th>Level of Resilience</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN-ORBIT TESTING</td>
<td>X</td>
</tr>
<tr>
<td>SUPPORT SERVICES AFTER ACCEPTANCE</td>
<td>X</td>
</tr>
<tr>
<td>TITLE/RISK TRANSFER</td>
<td>X</td>
</tr>
<tr>
<td>INITIAL/FINAL ACCEPTANCE</td>
<td>X</td>
</tr>
<tr>
<td>INITIAL/FINAL HANOVER</td>
<td>X</td>
</tr>
<tr>
<td>LIABILITY AFTER ACCEPTANCE</td>
<td>X</td>
</tr>
<tr>
<td>DUTY TO CORRECT</td>
<td>X</td>
</tr>
<tr>
<td>IO56 PERFORMANCE INCENTIVE</td>
<td>X</td>
</tr>
<tr>
<td>SECURITY FOR PERFORMANCE INCENTIVE</td>
<td>X</td>
</tr>
<tr>
<td>PENALTIES</td>
<td>X</td>
</tr>
<tr>
<td>FORCE MAJEURE</td>
<td>X</td>
</tr>
<tr>
<td>WARRANTIES</td>
<td>X</td>
</tr>
<tr>
<td>HARDSHIP</td>
<td>X</td>
</tr>
<tr>
<td>INSURANCE</td>
<td>X</td>
</tr>
<tr>
<td>DISPUTE RESOLUTION/ARBITRATION</td>
<td>X</td>
</tr>
<tr>
<td>BACK-UP LAUNCH SERVICES</td>
<td>X</td>
</tr>
<tr>
<td>CROSS-WAIVERS</td>
<td>X</td>
</tr>
<tr>
<td>LIABILITY DURING EXECUTION</td>
<td>X</td>
</tr>
<tr>
<td>LIABILITY AFTER EXECUTION</td>
<td>X</td>
</tr>
<tr>
<td>PROTECTED TRANSPONDERS</td>
<td>X</td>
</tr>
</tbody>
</table>
RESILIENSIS SPATIALIS CONTINUED HARD

FINDING: OF ALL STUDIED CLAUSES, 25% ONLY = SERVICE ASSURANCE. CONTRACTS TODAY ARE NOT RESILIENT.

A DEFINITION

For the interpretation or implementation of this Article:

- “Resilience” refers to the ability of a [satellite system / launcher / transponder / signal ...], faced with an Event or a Combination of Events that modifies its Essential Functionality,
- to spontaneously reduce the amplitude and duration of its effects, and, (Continued)
- to return instantaneously to stable operating conditions, involving only limited and objectively acceptable degradations

“Essential Functionality” means the functionality of the [Satellite System / Launcher / Repeater / Signal [...] corresponding to the Resilience Level, described in the Annex below (Annex “Resilience”)

- “Level of Resilience” means the level of resilience chosen by the Customer, corresponding to the Essential Functionalities of the [satellite system / launcher / transponder / signal [...] as described in the annex below (Annex “Resilience”)

- “Events or combination of events” means the following events or combinations of events: Events affecting hardware [...] Events affecting the software [...] Firmware Events: [...] (Continued)

- “Stable operating conditions” means the following conditions, as measured as indicated below. [...] (Continued)
- “Limited and objectively acceptable degradations” means the degradations listed below [...] (Continued)

A CLAUSE

The Supplier undertakes, subject to the sanctions and incentives described below, to take all precautions or measures useful to the guarantee of the Level of Resilience and more particularly, to design, manufacture, procure or procure, subcontract, assemble, operate, provide, maintain, monitor ... the [satellite system / launcher / repeater / signal [...] subject of this contract, in such a way that, in the event of the occurrence of an event or a combination of events that would modify its essential functionalities, whether these events or event combinations affect the hardware, the software or that they originate from a firmware defect, their amplitude and the duration of their effects are spontaneously reduced, and the [satellite system / launcher / repeater / signal [...] (Continued) returns to stable operating conditions, involving only limited and objectively acceptable degradations.
Contracts? Innovation and systems

Reality is made up of circles, but we see straight lines. Herein lies the beginnings of our limitations as systems thinkers.

The Fifth Discipline: The Art & Practice of The Learning Organization: Peter M. Senge
/picture from the Arrival film (D. Villeneuve)
3. RESILIENCE: SPACE SYSTEMS THINKING

- Resilience
- Resourcefulness
- Rapidity
- Redundancy
- Robustness (Bruneau’s 4 Rs)
- Recover
- Respond
- Remember

ROI?
“THE DEAL OF THE YEAR”

• EX: Paradigm Secure Communications and UK MoD:
  • Invest less in insurance and more in resilience:
  • “Pay for assurance of service rather than pay for insurance.”
  • A successful story where a PPP was transformed from within:
    • The parties agreed thanks to the contractual flexibility to build spare satellites instead of investing further into insurance.
    • Launched and replacement ➔ active in orbit = more resilient signal, more infrastructure and service resilience, more business opportunity.
  • Reimbursed banks early and made more profits.

Problem with PPPs = Pandora Box.
(CIs interests: public ≠ private.
(Paradigm = success because of flexible contract and will of the parties.)
Recover and:

- **Adapt**
  
  Ecology: *progressive view* = adapt to new equilibrium (multi stable states = ecosystemS, polycentricity). **RESILIENT**
  
  $\rightarrow$ // **EQUITY** (FLEXIBLE), accommodating the adaptive capacity of law

- And/or

- **Return**
  
  Engineering: *conservative view* = recover to initial equilibrium (one state). **RESISTANT**
  
  $\rightarrow$ // **STARE DECISIS** (LINEAR)
4. **RESILIENSIS SPATIALIS: A MODEL OF RECOMMENDATIONS**

Combination of **hard** and **soft** resilience:

**HARD RESILIENCE - OUTCOME**
- Recover to *initial/adapt to new* equilibrium
- Technical requirements
- **Contractual clauses** and flexibility, no more battle of SLAs

**SOFT RESILIENCE – PROCESS**
- Adapt to *new* equilibrium
- Organizational management
  - Adaptive and polycentric governance
  - (shadow heterarchy, *metagovernance*, HR, context fostering flexible contracts)
RESILIENSIS SPATIALIS continued SOFT

ORGANIZATIONAL CULTURE… THE WILL

ADAPTIVE (META) GOVERNANCE,
CO-MANAGEMENT
POLYCENTRICITY
WHERE NEXT?

• Unchartered territory

• UNIDROIT?

• WORKING GROUP?
  (Academic institutions, Private foundations, Industry, International associations and Space agencies)

• LTS Guidelines (UNISPACE 50)?

• International conferences (e.g. UNIDIR, IAF Space Security, etc.)

Any suggestions? Thank you! Maria.lucas-rhimbassen@ut-capitole.fr