RESILIANCE OF CRITICAL INFRASTRUCTRURES

The need for Private-Public Partnerships



Richard Krock

Bell Labs

15 September, 2009

All Rights Reserved © Alcatel-Lucent 2009

Agenda

1. Analyzing Infrastructures
2. The ARECI Study and Report
3. On-going Activities

All Rights Reserved © Alcatel-Lucent 2009

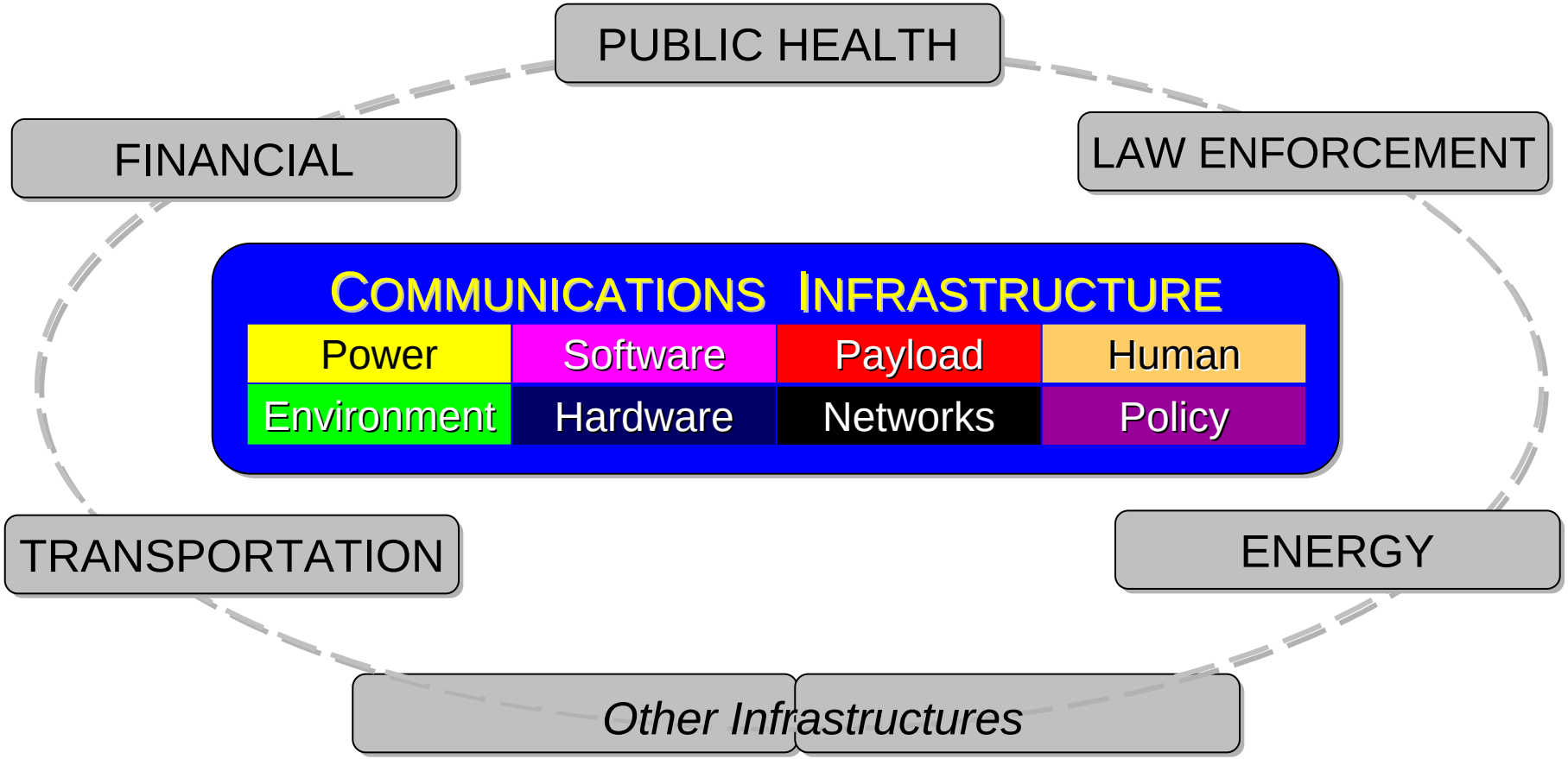
1 Analyzing Infrastructures

Threats vs. Vulnerabilities and the 8 Ingredients

All Rights Reserved © Alcatel-Lucent 2009

Critical Infrastructures

A communications point of view



All Rights Reserved © Alcatel-Lucent 2009

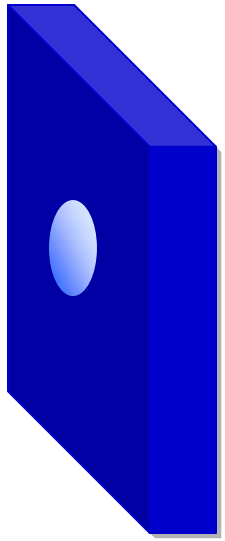
Threats & Vulnerabilities – different sides of an equation

Threat

Anything with the potential to damage or compromise the communications infrastructure or some portion of it

Vulnerability

A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise



All Rights Reserved © Alcatel-Lucent 2009

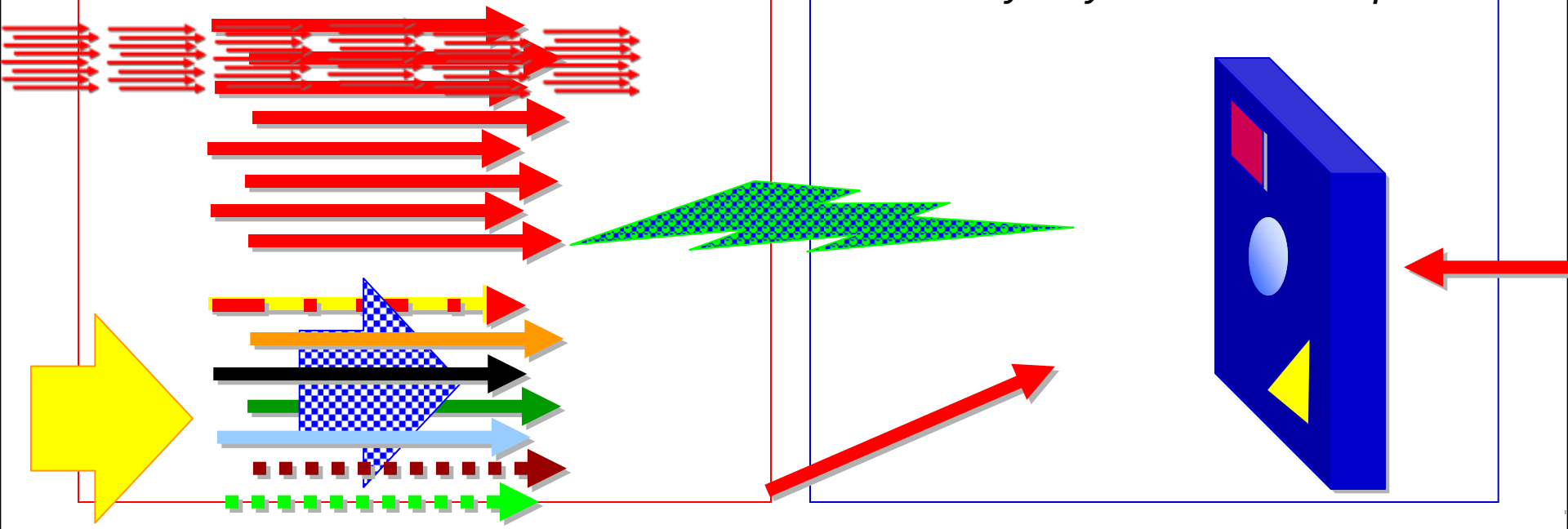
Characteristics of Ts and Vs

Threat

- *~ infinite in number*
- *knowledge value is fleeting*
- *each has permutations*

Vulnerability

- *finite*
- *fixed and well known*
- *only way threats can impact*



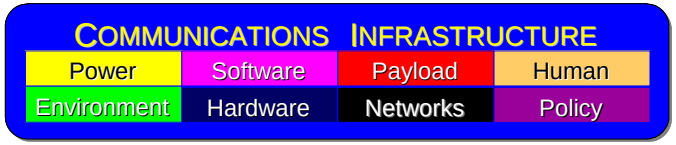
All Rights Reserved © Alcatel-Lucent 2009

A fundamental lesson . . .

. . . is the need to identify and address vulnerabilities – independent of threat knowledge

Does NOT mean that you abandon threat and risk analysis

It means you MUST supplement it, balance it, integrate it.



All Rights Reserved © Alcatel-Lucent 2009

8 Ingredient Framework

VULNERABILITY
uncontrolled fuel combustion
fuel contamination
fuel dependency
battery combustion
battery limitations
battery duration
maintenance dependency
require manual operation
power limitations
frequency limitations
susceptibility to spikes
physical destruction

VULNERABILITY
ability to control (render a system in an undesirable state, e.g
accessibility during development (including unsec
accessible distribution channels (interception)
accessibility of rootkit to control kernal/core
developer loyalties
errors in coding logic
complexity of programs
discoverability of intelligence (reverse engineer, exploi
mutability of deployed code (patches)

VULNERABILITY
unpredictable variation
extremes in load
corruption
interception
emulation
encapsulation of malicious content
authentication (mis-authenticaton)
insufficient inventory of critical compo
encryption (prevents observablity)

VULNERABILITY
physical (limitations, fatigue)
cognitive (distractibility, forgetfulness, ability to deceive, confusion)
ethical (divided loyalties, greed, malicious intent)
user environment (user interface, job function, corporate culture)
human-user environment interaction

COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

VULNERABILITY
accessible
exposed to elements
dependence on other infrastrucu
contaminate-able
subject to surveillance
continuously being altered
identifiable
remotely managed
non-compliance with established

VULNERABILITY
chemical (corrosive gas, humidity, temperature, cor
electric (conductive microfiber particles – carbon bc
radiological contamination
physical (shock, vibration, strains, torque)
electromagnetic energy (EMI, EMC, ESD, RF, EMP
environment (temperature, humidity, dust, sunlight,
life cycle (sparing, equipment replacement, ability to
logical (design error, access to, self test, self shut off)

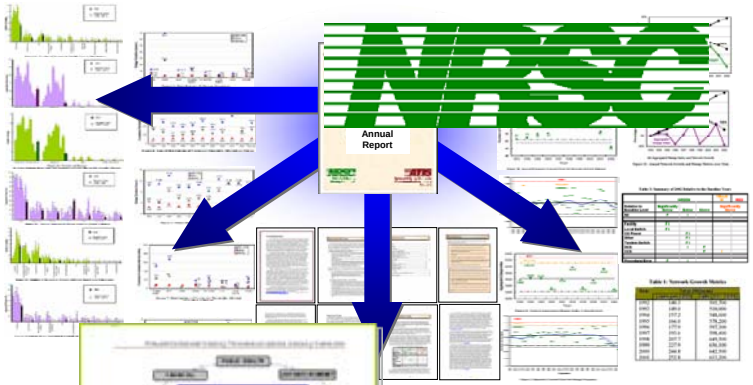
VULNERABILITY
capacity limits
points or modes of failure
points of concentration (congestion)
complexity
dependence on synchronization
interconnection (interoperability, interdependence
uniqueness of mated pairs
need for upgrades and new technology
automated control (*via software)
accessibility (air, space or metallic or fiber)
border crossing exposures

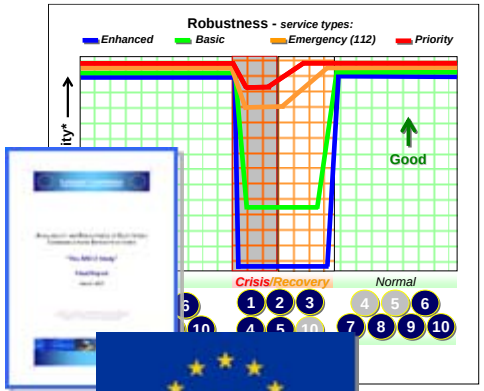
VULNERABILITY
Lack of ASPR (agreements, standards, policies, regulations)
Conflicting ASPR
Outdated ASPR
Unimplemented ASPR (complete or partial)
Interpretation of ASPR (mis- or multi-)
Inability to implement ASPR
Enforcement limitations
Boundary limitations
Pace of development
Information leakage from ASPR processes
Inflexible regulation
Excessive regulation
Predictable behavior due to ASPR
ASPR dependence on misinformed guidance
ASPR ability to stress vulnerabilities
ASPR ability to infuse vulnerabilities
Inappropriate interest influence in ASPR

All Rights Reserved © Alcatel-Lucent 2009

8 Ingredient Framework and Private Public Partnerships





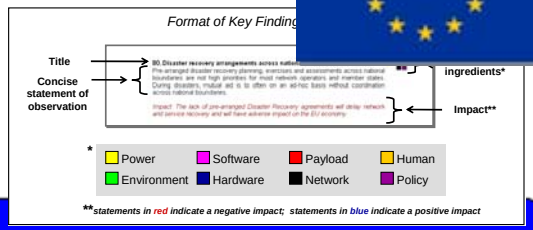




WIRELESS EMERGENCY RESPONSE TEAM







COMMUNICATIONS INFRASTRUCTURE

Power	Software	Payload	Human
Environment	Hardware	Networks	Policy

The Eight Ingredient Framework has been used by numerous critical industry-government collaborative fora, engaging over one thousand subject matter experts.

All Rights Reserved © Alcatel-Lucent 2009

Best Practices, Standards or Regulations ?

Regulations

- legal process; technical expertise may be compromised
- speed: **S L O W** t o a d j u s t
- posture: mandated behavior

Standards

- competitive process; influence of strongest competitor wins
- speed: **M E D I U M t o a d j u s t**
- posture: ranges from voluntary to mandated

Best Practices

- expert process; expertise and experience are trump
- speed: *FAST to adjust*
- posture: implementation is voluntary

All Rights Reserved © Alcatel-Lucent 2009

2 The ARECI Study and Report

All Rights Reserved © Alcatel-Lucent 2009

EC ARECI Study – Executive Summary

Summary Statistics



10 Recommendations

25 Member expert team conducted study

71 European-confirmed Best Practices

81 Intrinsic vulnerabilities considered

100 Key Findings

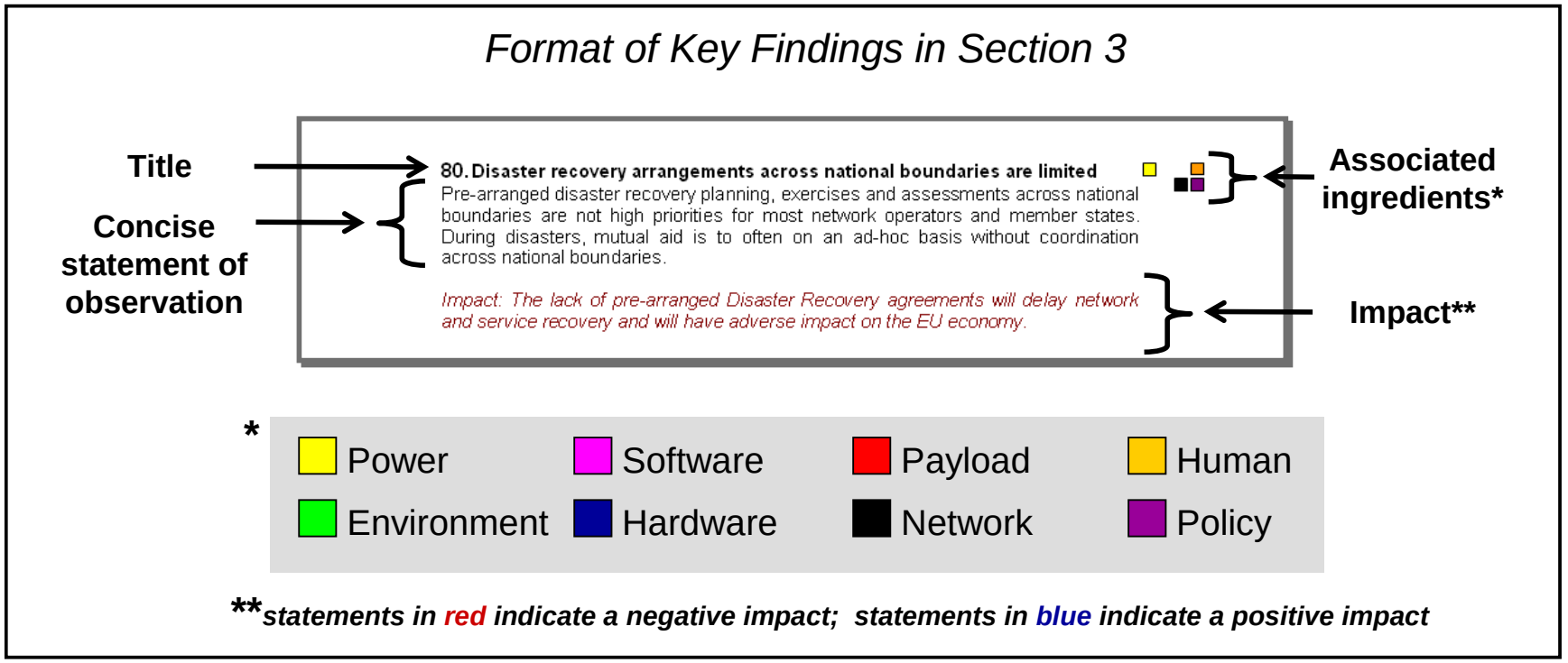
150 Contributing European stakeholder experts

200+ Critical trends considered for impact

30,000+ Distinct data points researched and analyzed during study

All Rights Reserved © Alcatel-Lucent 2009

The 8 Ingredient Framework introduces meaningful linkages . . .

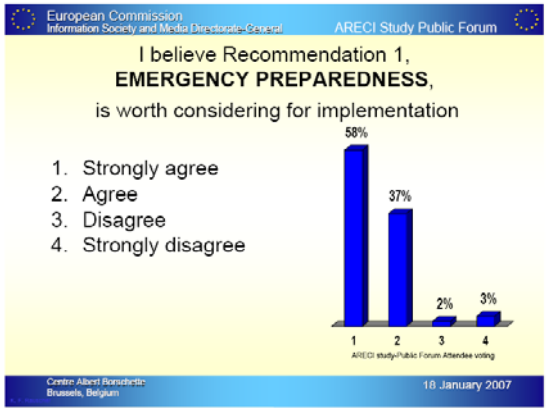


All Rights Reserved © Alcatel-Lucent 2009

10 Recommendations

1. Emergency Preparedness
2. Priority Communications on Public Networks
3. Formal Mutual Aid Agreements
4. Critical Infrastructure Information Sharing
5. Inter-Infrastructure Dependency
6. Supply Chain Integrity and Trusted Operation
7. Unified Voice in European Standards
8. Interoperability Testing
9. Vigorous Ownership of Partnering Health
10. Discretionary European Expert Best Practices

86% of stakeholders agree or strongly agree



All Rights Reserved © Alcatel-Lucent 2009


Recommendation 1
Emergency Preparedness

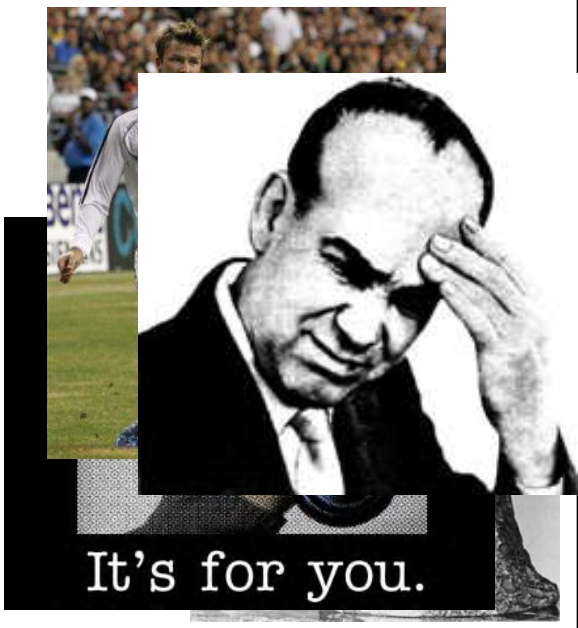
1. Emergency Preparedness

Issues

- Disasters are infrequent events – FORTUNATELY!
- Formal disaster plans are lacking
- Priority restoration plans are not widely in place

Alternative Approaches

- “If Beckham doesn’t need to practice, neither do I”
- “I’ve got a pretty good idea what to do”
- “I’ve got a contact I can call”
- “We’ll figure out what to restore first once we see what’s out”



All Rights Reserved © Alcatel-Lucent 2009

1. Emergency Preparedness

The Private Sector and Member State governments should jointly expand their use of emergency exercises and establish pre-arranged priority restoration procedures for critical services to better meet the challenges of inevitable emergency incidents.

All Rights Reserved © Alcatel-Lucent 2009

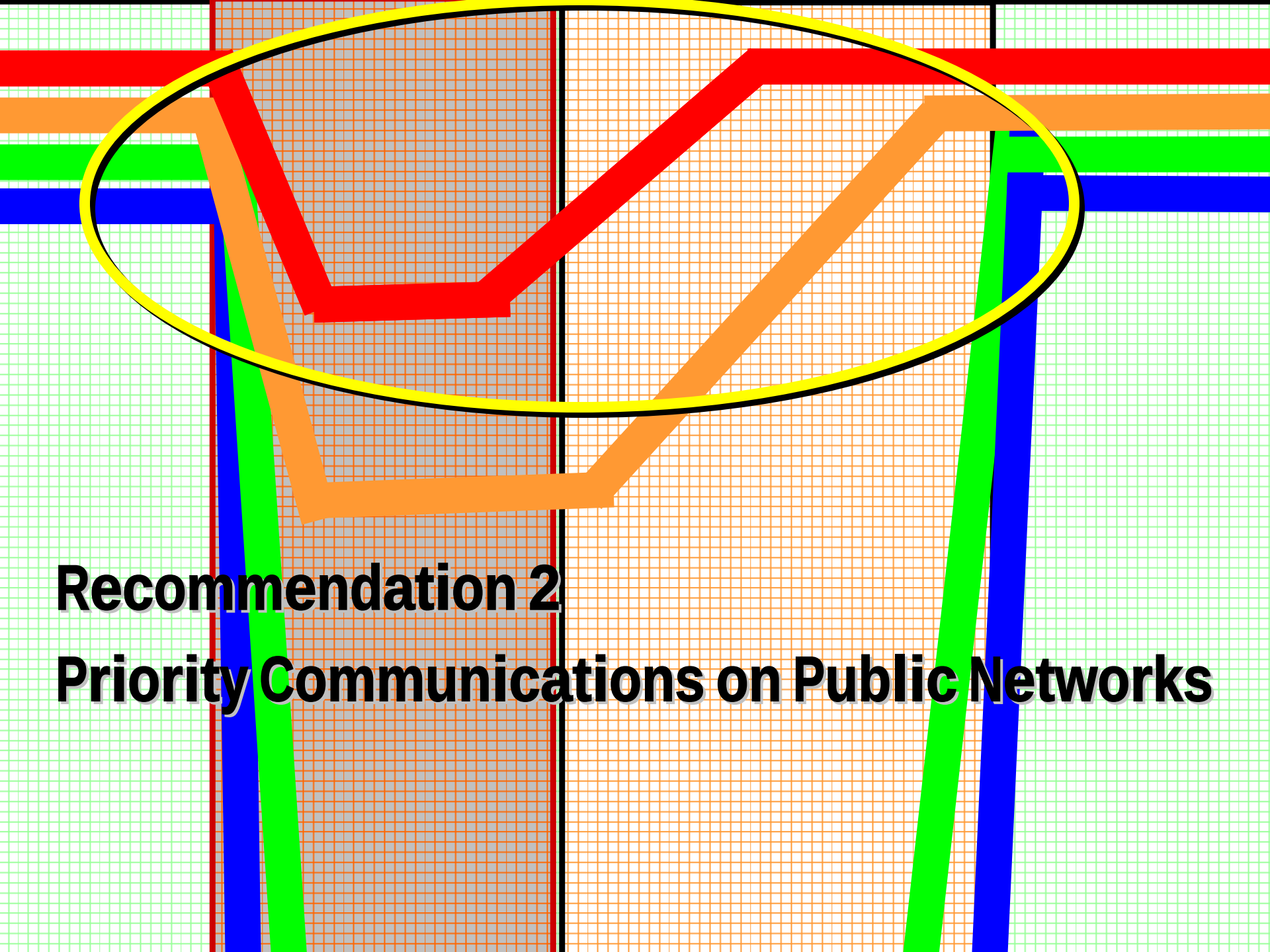
1. Emergency Preparedness

1-1. The Private Sector and Member State governments should jointly convene to review recent emergency situations and develop a list of lessons learned.

1-2. The Private Sector and Member State governments should jointly conduct periodic emergency exercises that include multiple members within the industry, other infrastructures, and multiple Member States

1-3. Member State governments and the Private Sector should meet to review current regulations that may govern priority restoration, and develop a formal plan for pre-identifying critical services and providing priority restoration for those services.

All Rights Reserved © Alcatel-Lucent 2009



Recommendation 2

Priority Communications on Public Networks

2. Priority Communications on Public Networks

Issues:

Some communications absolutely must complete:

- even in times of crisis
- even during massive overloads
- even when parts of the network are service



Alternative Approaches

- "All calls are priority"
- "We rely on our private network."
- "We only need to talk to people on the private netwc
- "We'll figure out a way to communicate across the border if we have to"

All Rights Reserved © Alcatel-Lucent 2009

2. Priority Communications on Public Networks

Member State governments should implement a standards-based priority communications capability on future public networks in order to ensure vital communications for critical government authorized callers. This public network capability is needed in addition to any private emergency networks that already exist and should not be viewed as a substitute or replacement for such private networks.

All Rights Reserved © Alcatel-Lucent 2009

2. Priority Communications on Public Networks

Suggested Next Steps

2-1. Member States to create and provide specific mission based needs descriptions for priority calling.

2.2 Private Sector and Member State regulatory bodies convene for the purpose of agreeing on standards for priority calling on public networks.

2.3 Member States allocate funds for the deployment of priority calling over public networks.

2.4 Equipment suppliers implement the agreed priority calling functionality in their products.

2.5 Private Sector network operators deploy priority calling features in their networks.

All Rights Reserved © Alcatel-Lucent 2009

Recommendation 4
Critical Infrastructure Information Sharing

4. Critical Infrastructure Information Sharing

Issues

- The government has sensitive information that could help the communications industry
- The communications industry has sensitive information that could help the government
- Information sharing that does occur is largely informal



Alternative Approaches

- “I’ll decide who I’ll share with
- “You don’t need to know ”
- “If you aren’t going to tell me on your own, I’ll make you tell me”
- “We’ll gather all the sensitive information and keep it safe here”

All Rights Reserved © Alcatel-Lucent 2009

4. Critical Infrastructure Information Sharing

Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe.

All Rights Reserved © Alcatel-Lucent 2009

4. Critical Infrastructure Information Sharing

4-1. The Private Sector and Member State stakeholders should investigate, and where appropriate, join some of the excellent information sharing organizations that already exist.

4-2. The Private Sector and the Member State stakeholders should convene to establish a trusted environment for information sharing within each Member State, both from industry to government and from government to industry.

4-3. Member States governments should identify those information sharing models which will best enable the sharing of threat and other sensitive information across Member State boundaries. These models should be implemented, if they do not already exist, and this information should then be shared, as appropriate, with industry partners within those Member States.

All Rights Reserved © Alcatel-Lucent 2009

10 ARECI Recommendations

Directed to . . .

Table 4: Summary of Required Leadership Posture

Recommendation	Private Sector	Member States	European Institutions
1	L	AS	AS
2	AS	L	AS
3	L	AS	AS
4	AS	L	
5	AS	L	AS
6	L	L	L
7	AS	L	AS
8	L	AS	AS
9	L	L	L
10	L	AS	AS

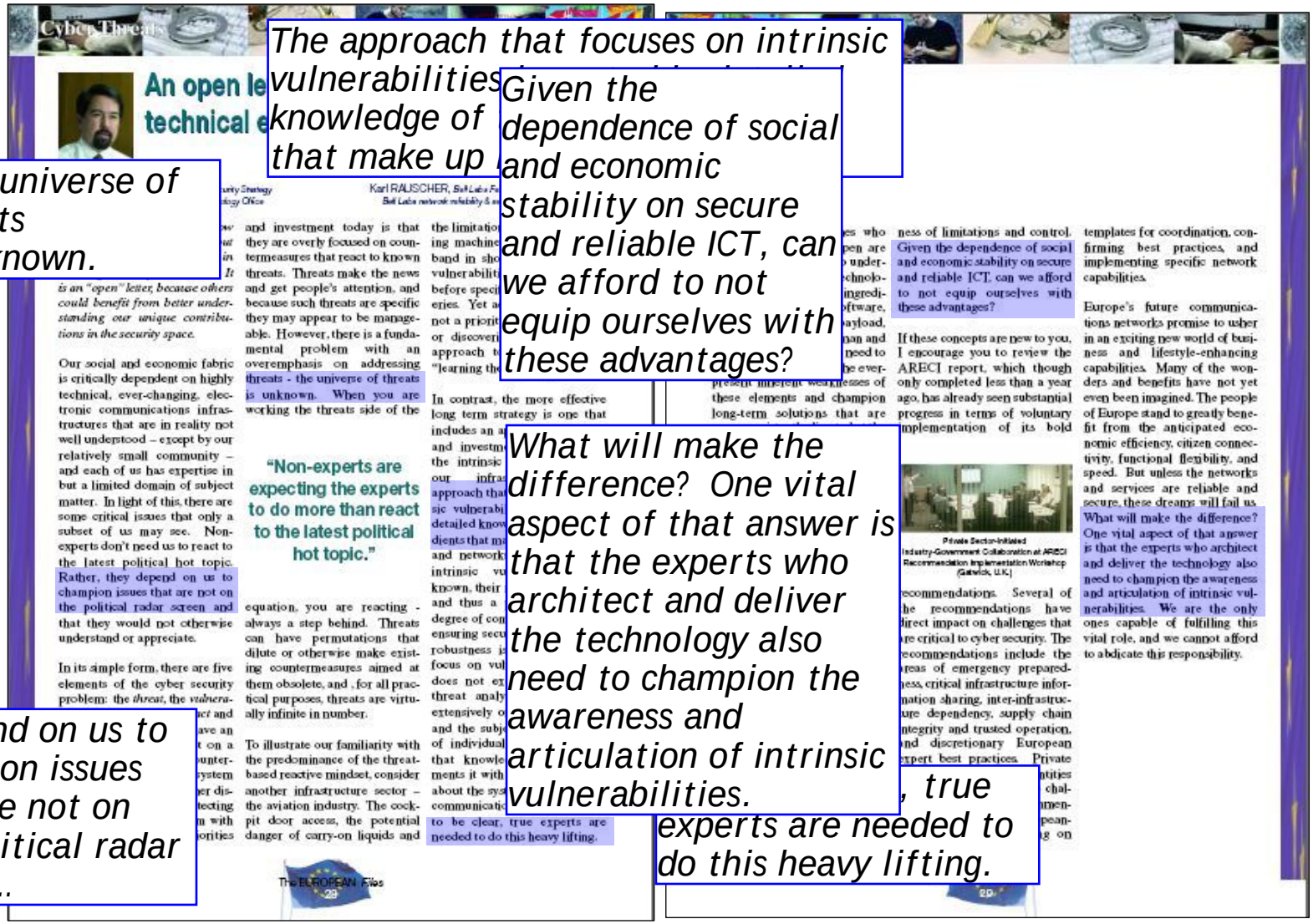
Key:	
AS	*Active supporter*
L	*Primary leader*

All Rights Reserved © Alcatel-Lucent 2009

3 On-going Activity

All Rights Reserved © Alcatel-Lucent 2009

An open letter to Europe's technical experts



…the universe of threats is unknown.

The approach that focuses on intrinsic vulnerabilities knowledge of that make up

Given the dependence of social and economic stability on secure and reliable ICT, can we afford to not equip ourselves with these advantages?

What will make the difference? One vital aspect of that answer is that the experts who architect and deliver the technology also need to champion the awareness and articulation of intrinsic vulnerabilities.

…depend on us to champion issues that are not on the political radar screen…

…, true experts are needed to do this heavy lifting.

All Rights Reserved © Alcatel-Lucent 2009

AVAILABILITY AND ROBUSTNESS OF ELECTRONIC COMMUNICATIONS INFRASTRUCTURES

European Commission
Information Society and Media Directorate-General

"The ARECI Study"

European Commission
Information Society and Media Directorate-General

Final Report

March 2007



Priority Communications

Slovakia

Emergency Preparedness

Mutual Aid

Information Sharing

Government/Private Sector Partnership

Best Practices

Gatwick Workshop

Schipol Workshop

Portela Workshop



Information Sharing

Industry-Government Pandemic Information Sharing Conference Calls



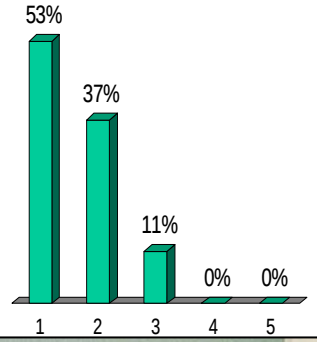
All Rights Reserved © Alcatel-Lucent 2009

Alcatel·Lucent



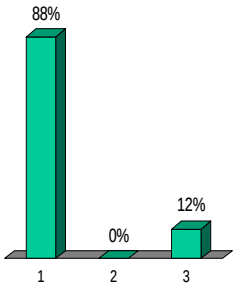
Taken as a whole, the two workshops were worth the time I spent

1. Strongly agree
2. Agree
3. Neither agree or disagree
4. Disagree
5. Strongly disagree



My organisation will take some action because of this workshop

1. Yes
2. No
3. Don't know



Industry and government meeting to implement ARECI recommendations







What does it take?

- Willingness of both sides
- Trust
- Time – so get started NOW!

Βοήθα με να σε βοηθώ ν' ανεβούμε το βουνό.

All Rights Reserved © Alcatel-Lucent 2009

The ROGUCCI Global Summit is being convened to assess:

- the reliability of undersea cable infrastructure at a global level,
- the potential impacts of infrastructure failures–with financial sector focus, and
- proposed recommendations for improved global infrastructure resilience.

All Rights Reserved © Alcatel-Lucent 2009

Day 1 - Technical Experts examining the Intrinsic Vulnerabilities

- What has happened
- What hasn't happened yet

Day 2 – Financial Sector

- The Impact of undersea cable damage
- Stephen Malphrus, Chief of Staff – US Federal Reserve Board
- Expert Panel

Day 3 – Summit Council

- Experts review proceedings from Days 1 & 2 and determine strategy going forward

All Rights Reserved © Alcatel-Lucent 2009

"A Conversation on Information and Communications Infrastructure Dependability"

Facilitated by IEEE Communications Society

- beginning as a CEO-level periodic meeting
- senior government stakeholders to be added
- aim is to further the advancement of Private Public Partnerships
- Examples of topics
  - Formal mutual aid agreements
  - New international cooperation on the resilience of global undersea cable infrastructure
  - Best Practices (e.g., Pandemic Information Sharing, Emergency Preparedness)
  - Progress in growth of trusted information sharing communities
  - Standards-based priority communications over public networks

All Rights Reserved © Alcatel-Lucent 2009

www.alcatel-lucent.com

www.bell-labs.com/ARECI

http://community.comsoc.org/groups