A Formula for Network Resilience

David Hutchison

Lancaster University

d.hutchison@lancaster.ac.uk

GFI Summit, Seoul, 20 Nov 2013

LANCASTER UNIVERSITY InfoLab21

Resilience

Generally, this means the capability of people to ‘bounce back’ after experiencing problems [Oxford English Dictionary definition: “Power of resuming the original form after compression &c.”]

Specifically, a resilient system is one that can continue to offer a satisfactory level of service even in the face (or in the aftermath) of the challenges it experiences

Resilience goes beyond security; it encompasses security but aims to recover from security breaches and also any other challenges that compromise the system

LANCASTER UNIVERSITY InfoLab21

Resilience as a network need

- Society is increasingly **reliant** on the Internet and on networked systems in general ('Information Society')
- Communication networks now underpin many of society's critical infrastructures
- We need **resilience**, a (QoS) property of networks and systems such that they can withstand any challenge, whether from natural disasters, mis-configurations, hardware or software failures, congestion/overloads (including flash crowds), or attacks
- Network system attacks are increasing in variety and number: virus, worms, botnets, DoS, …

"Future Internet Research: The EU framework" by Joao da Silva
"… as the Internet is increasingly becoming a "critical infrastructure, security and robustness of the Internet are naturally becoming issues of major concern." (ACM CCR, 2007)

acmqueue **"Resolved: the Internet Is No Place for Critical Infrastructure"** by Dan Geer | April 2, 2013

Chinese domains downed by 'largest ever' cyber-attack. DDoS attacks targeted the country's national registry. *The Independent,* Aug 27, 2013

It is no coincidence that every single major cloud storage provider went down last week. That's Google's cloud storage, Microsoft's cloud storage, Intel's cloud services and Amazon's (the biggest and used by a huge number of other providers from Dixons and Dropbox to Spotify). Remember these services are supposed to have a 99.999% availability yet they've all failed with one day of each other. Not a single word of explanation from any of the companies involved …

LANCASTER UNIVERSITY InfoLab21

European communication networks ‘incidents’ gathering

European Network and Information Security Agency

Annual Incident Reports 2012

Analysis of Article 13a annual incident reports

August 2013

www.enisa.europa.eu

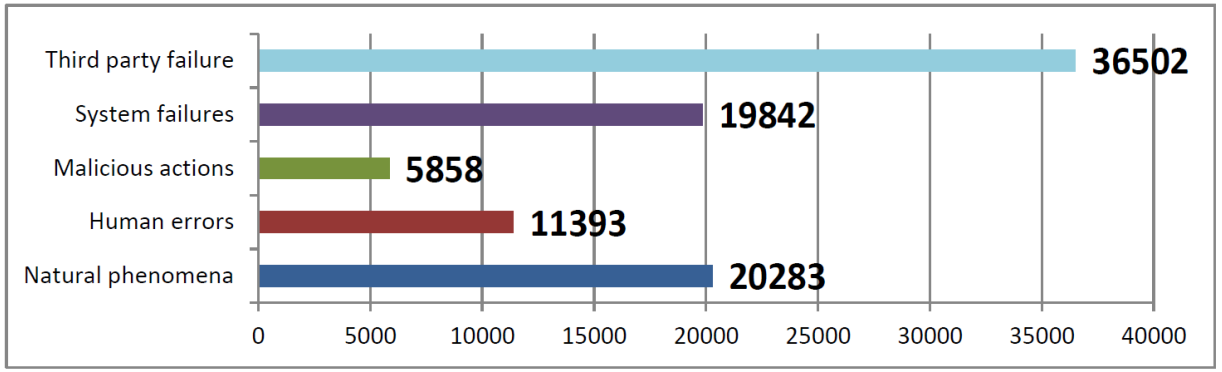


Figure 16 Average user-hours lost per incident per root cause category.

The incidents caused by third party failures affected most connections (around 2.8 Million)

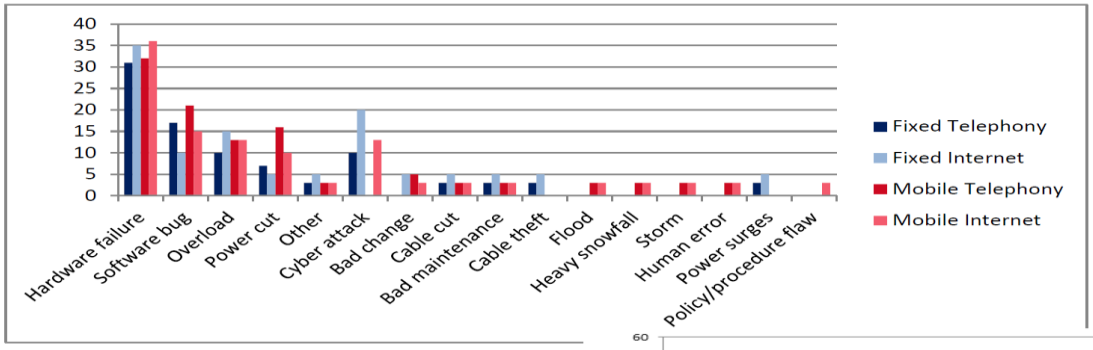
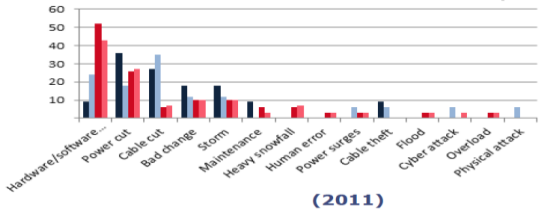


Figure 13 Detailed causes per service



Causes of incidents per service – hardware failure is the most common

Some notable past challenges

- 2001 Baltimore tunnel fire
- 2001 9/11 terrorist attacks
- 2003 Cogent peering disputes
- 2003 Northeast US blackout
- 2005 7/7 terrorist attacks
- 2005 Hurricane Katrina
- 2006 Hengchun earthquake
- 2008 Pakistan YouTube hijack
- 2008 Mideast submarine cable cuts
- 2009 H1N1 influenza pandemic
- 2010 Stuxnet worm attack

General lessons:

-Plan for vulnerabilities (threats may be predictable)

- Redundancy without diversity is not resilient

A crucial issue identified by ENISA is the lack of a standardised framework, even for the most basic resilience measurements. There are not many frameworks, none of them globally accepted.

LANCASTER UNIVERSITY InfoLab21

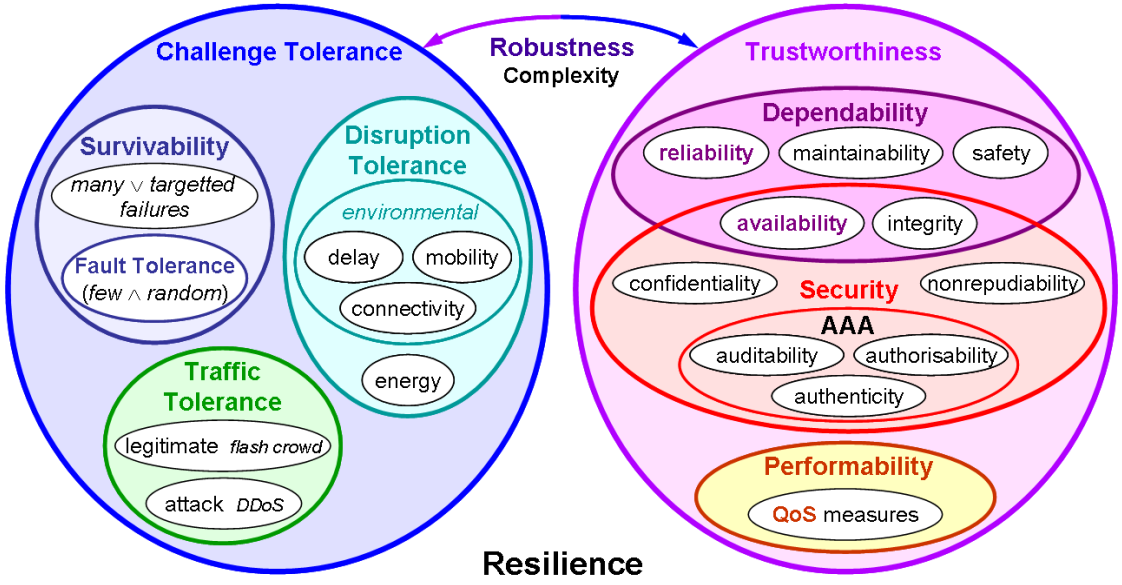
ResiliNets project (Kansas, Lancaster): to establish a framework for network resilience

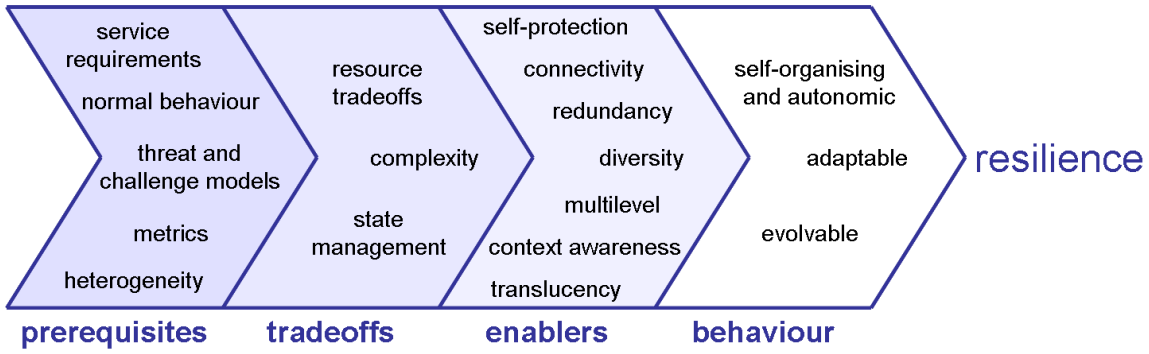
First, investigated the relationship between resilience and other previously-researched areas:

- **Disciplines related to faults and challenges**
  - Fault Tolerance
  - Survivability
  - Disruption Tolerance
  - Traffic Tolerance
- **Trustworthiness disciplines related to quantifiable properties**
  - Dependability
  - Security
  - Performability
- **Trustworthiness with respect to challenges**
  - Robustness.
  - Complexity

LANCASTER UNIVERSITY InfoLab21

Resilience properties and principles





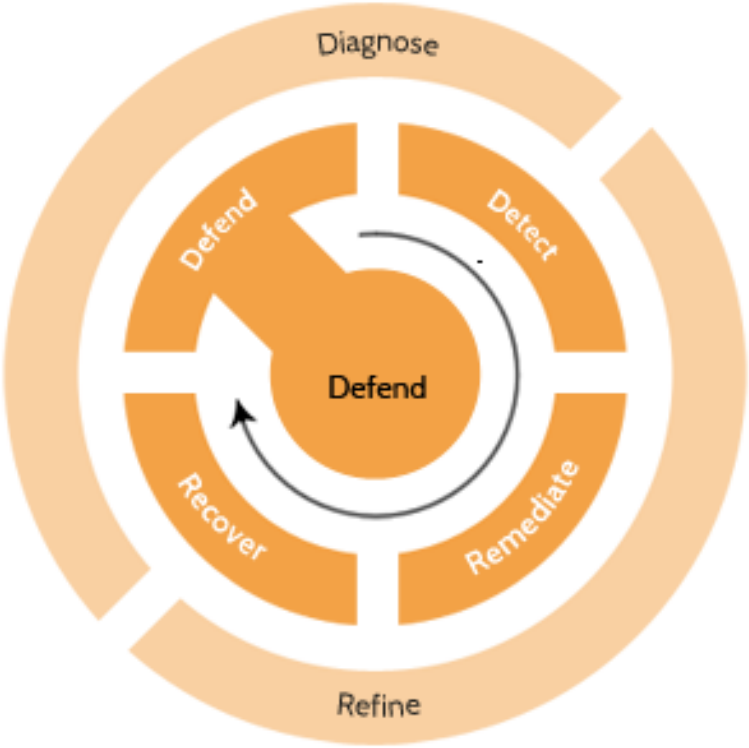
LANCASTER UNIVERSITY InfoLab21

ResiliNets “formula” and strategy

“D^2R^2+DR” → Resilience

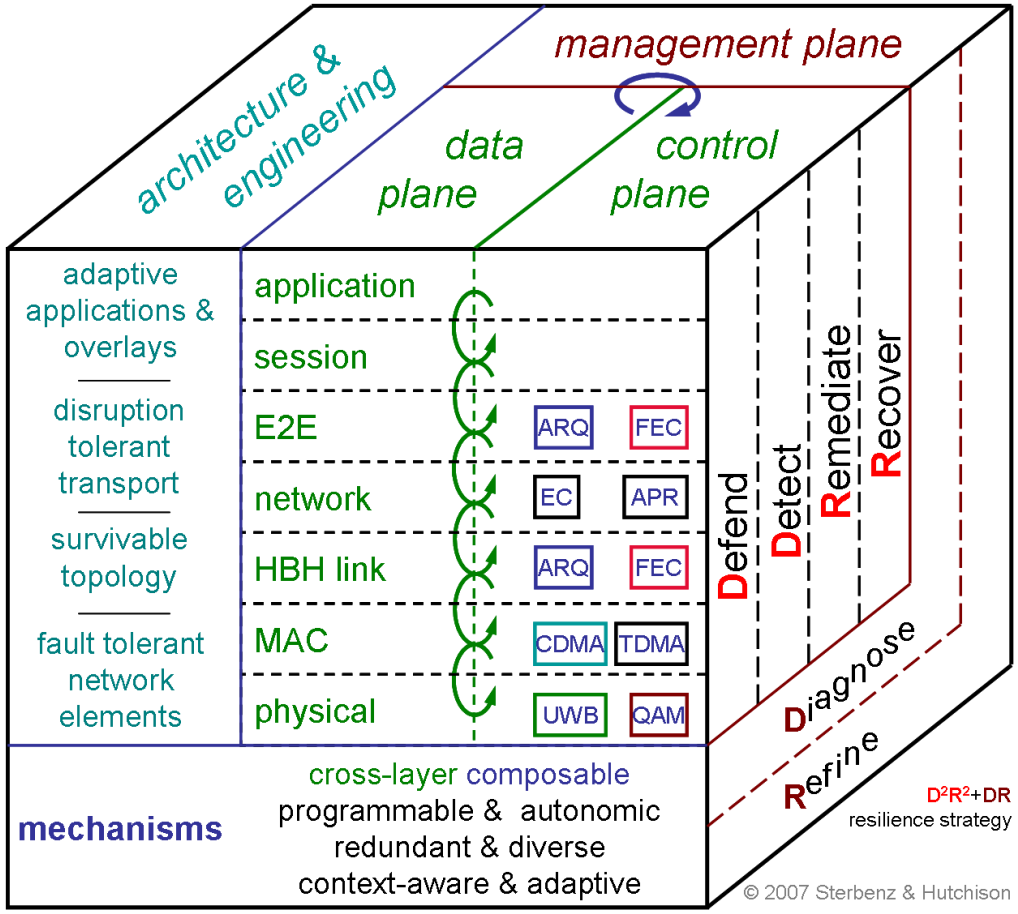
Real-time Control Loop
- **D**efend
- **D**etect
- **R**emediate
- **R**ecover

System Enhancement
- **D**iagnose
- **R**efine



LANCASTER UNIVERSITY InfoLab21

Resilience cube model



LANCASTER UNIVERSITY InfoLab21

The ResumeNet project (2008-2011): to evaluate the D^2R^2+DR resilience strategy

ETH Zürich (ETHZ) – coordinator	Switzerland
Lancaster University (ULanc)*	United Kingdom
Technical University Münich (TUM)	Germany
France Telecom (FT)	France
NEC Europe Ltd (NEC)	United Kingdom
Universität Passau (UP)	Germany
Technical University Delft (TUDelft)	Netherlands
Uppsala Universitet (UU)	Sweden
Université de Liège (ULg)	Belgium

* Also: the Universities of Kansas (USA) and Sydney (Australia)

LANCASTER UNIVERSITY InfoLab21

Approach: three conceptual levels

- **Framework**
  - Architecture
  - Information flow
  - Metrics
  - Challenge classification
- **Mechanisms and algorithms**
  - Network resilience (redundancy, diversity in routing, transport, incentives for collaboration, challenge detection)
  - Service resilience (overlays/P2P, virtualization, challenge detection, machine learning)
- **Validation** by experimentation in testbeds and with simulation
  - {network, service, challenge, resilience mechanism}
  - Realistic models, traffic and system behavior traces

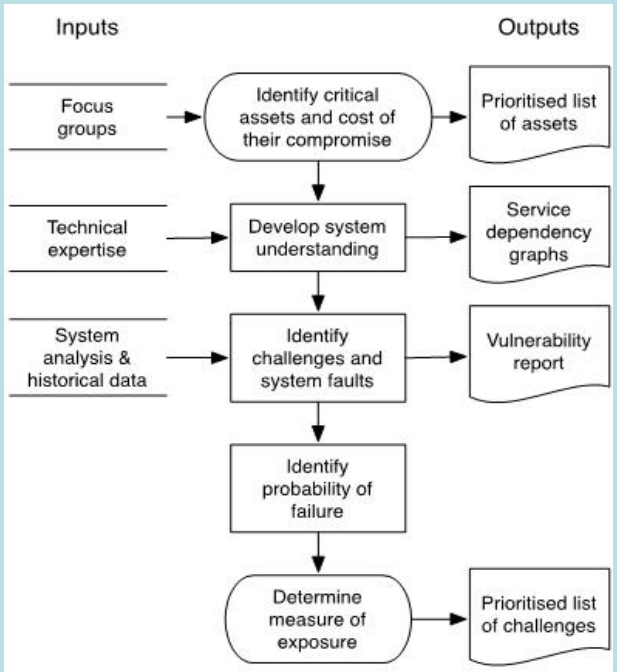
The ResumeNet framework was experimentally evaluated in Future Internet scenarios: wireless mesh networks; disruption tolerant networks; a multimedia service provisioning context; and in an Internet of Things environment

LANCASTER UNIVERSITY InfoLab21

De-constructing D^2R^2+DR (1)

- Defend: static, and dynamic
- Initially:
  - System analysis
  - Risk assessment
  - Prioritise the assets
  - Build defensive walls
  - E.g. redundant links, nodes
- Runtime:
  - Make adjustments as appropriate
  - E.g. adjust firewall rules, resources

Marcus Schoeller et al, “Assessing Risk for Network Resilience” (RNDM 2011)



LANCASTER UNIVERSITY InfoLab21

De-constructing D^2R^2+DR (2)

- Detect
- Implies a monitoring system
  - Instrument the network!
  - cf. the Knowledge Plane?
  - Aim to observe normal behaviour
  - Then look for anomalies / intrusions
- Employ suitable ADTs / IDSs
  - Classify the detected anomalies
  - Attempt a root cause analysis?

A Knowledge Plane for the Internet
David D. Clark et al, *SIGCOMM'03*

"To learn about and alter its environment, the knowledge plane must access, and manage, what the cognitive community calls *sensors and actuators. Sensors are entities that produce observations. Actuators* are entities that change behavior (e.g., change routing tables or bring links up or down). So, for instance, a knowledge application that sought to operate a network according to certain policies might use sensors to collect observations on the network, use assertions to determine if the network's behavior complies with policy, and, if necessary, use actuators to change the network's behavior."

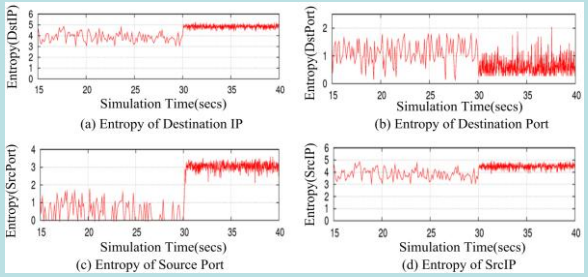


Fig. 5: Entropy changes with the Slammer Worm

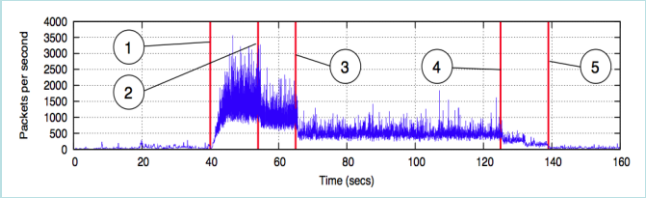
From: "PReSET: A Toolset for the Evaluation of Network Resilience Strategies", by Alberto Schaeffer-Filho et al *(IM 2013)*

LANCASTER UNIVERSITY InfoLab21

De-constructing D^2R^2+DR (3)

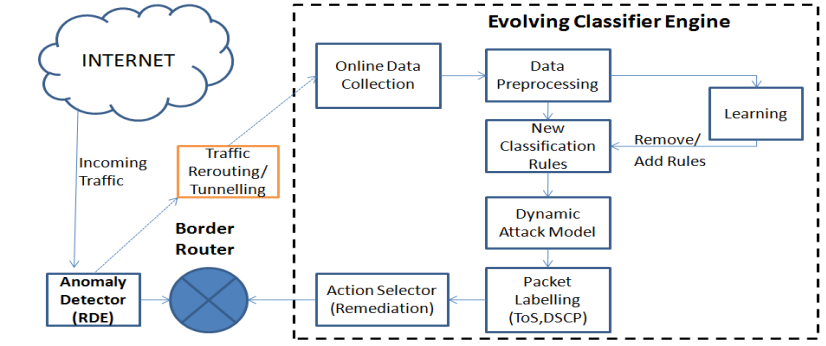
- Remediate
  - Rely on symptoms, or root cause
  - Typically use traffic engineering
  - Get as much context as possible
- Recover
  - Get back to normal behaviour if possible
  - Use policies for high-level guidance
- Diagnose & Refine
  - Learning phase
  - Human in the loop

Alberto Schaeffer-Filho et al, "Policy-based DDoS remediation" [see also DRCN 2011]



① Attack starts
② Rate limit the entire link
③ Rate limit all traffic towards the victim
④ Rate limit only the attack flow
⑤ Attack flows successfully classified

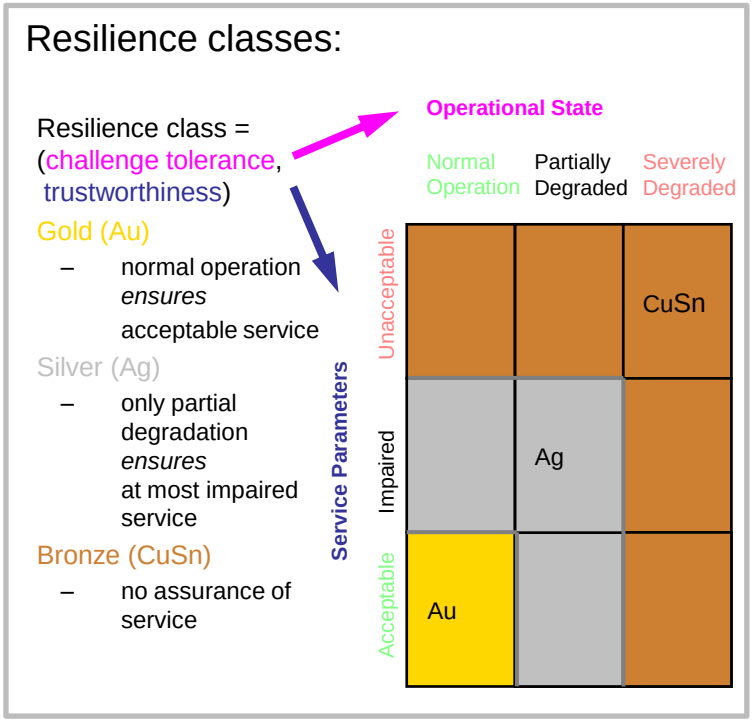
Azman Ali et al, "Evolving Classifier utilizing eClass0 and eCluster (ALS algorithms)"



LANCASTER UNIVERSITY InfoLab21

Resilience as a network metric

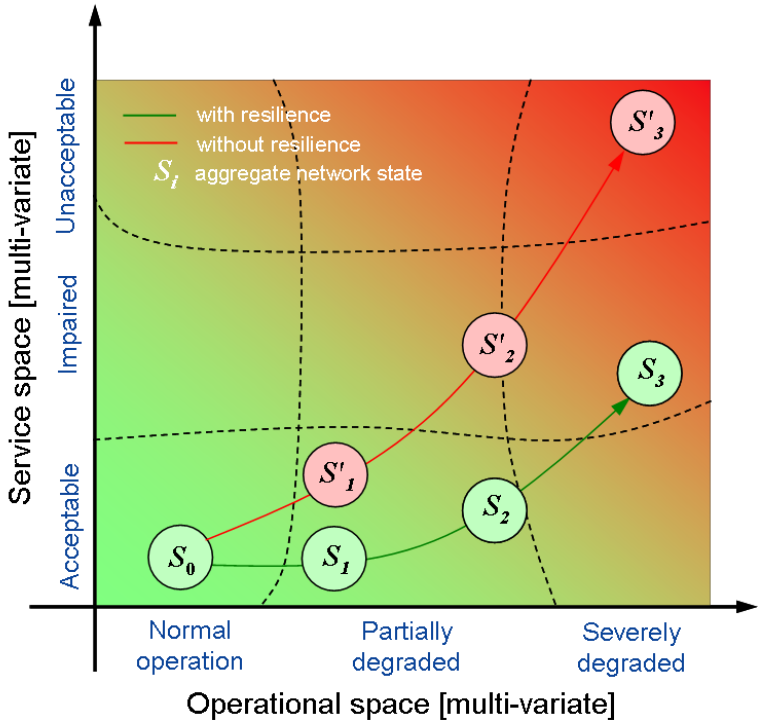
- We need to know how to specify resilience and how to measure it – i.e. the science and the engineering
- For computer networks, we should specify and measure resilience at the topology and the service levels
- Topology resilience: typically, structural diversity
- Service resilience: for example, a combination of availability and reliability
- Overall R [0,1]: a combination of individual metrics, maybe simplified as a set of ‘resilience classes’



LANCASTER UNIVERSITY InfoLab21

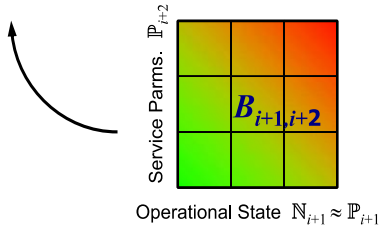
Resilience state space representation

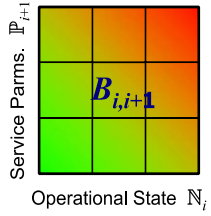
- Operational space **N**: represents the physical state of the network
  Resilient networks remain in normal operation in the face of challenges
  - **normal operation** according to network design and engineering
  - **partially degraded** but still operable
  - **severely degraded** providing little or no operational capability
- Service space **P**: represents the quality of service for an application over a given network
  Resilient services remain acceptable even with network operation degrades
  - **acceptable** service with respect to service specification
  - **impaired** but usable service
  - **unacceptable** service that provides little or no utility
- Resilience **R**: as a function of state transition probability in two-dimensional state-space:
  - network state ***S*** is discrete set of operational metrics and service parameters
  - aggregate network state

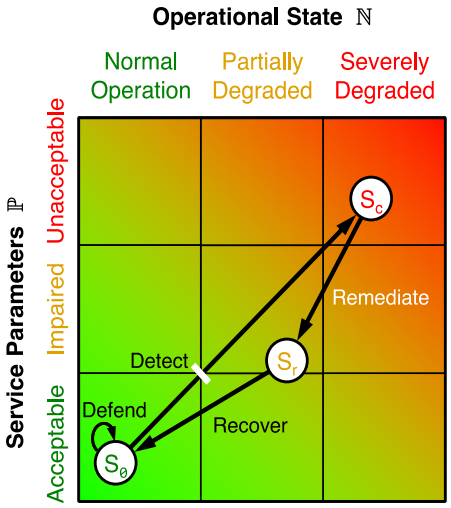


LANCASTER UNIVERSITY InfoLab21

Multilevel resilience and metrics

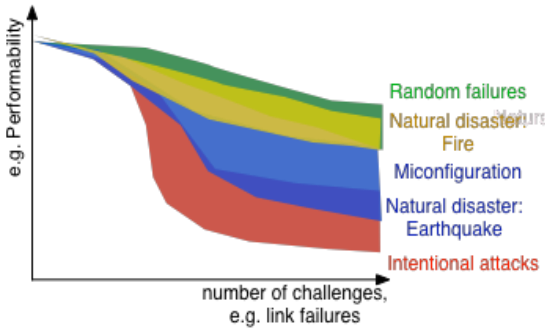


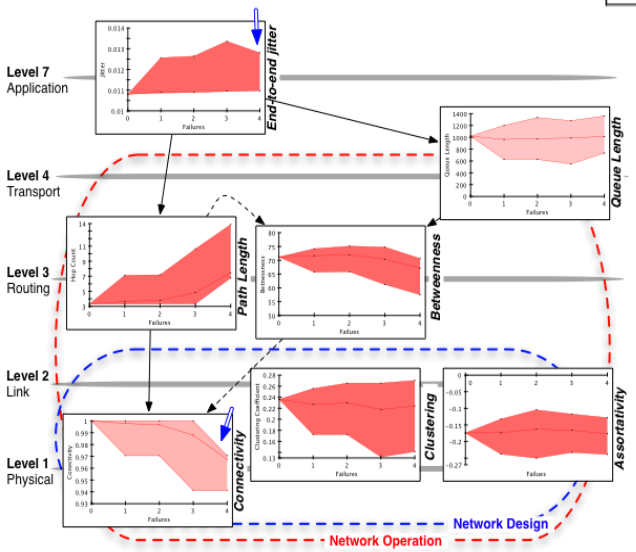




Comparing resilience based on **metric envelopes** gives a visual explanation of the network degradation process

The effect of various failure sources on the metric being evaluated can be revealed



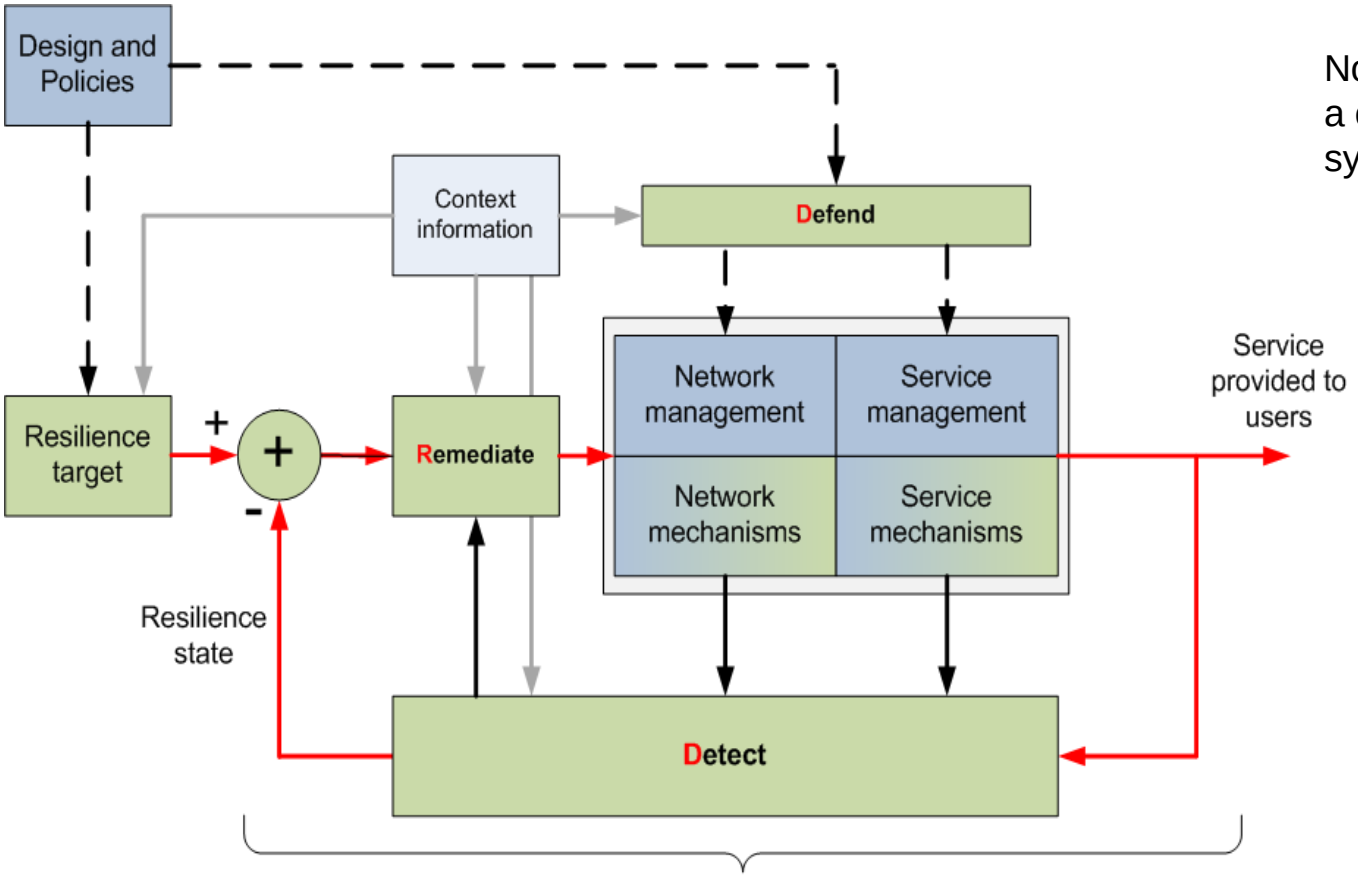


James PG Sterbenz et al, "Redundancy, Diversity, and Connectivity to Achieve Multilevel Network Resilience, Survivability, and Disruption Tolerance" (Telecommunications Systems Journal, 2012)

C. Doerr, and J. Martin-Hernandez, "A computational approach to multi-level analysis of network resilience" (DEPEND 2010)

LANCASTER UNIVERSITY InfoLab21

ResumeNet architectural model: D^2R^2

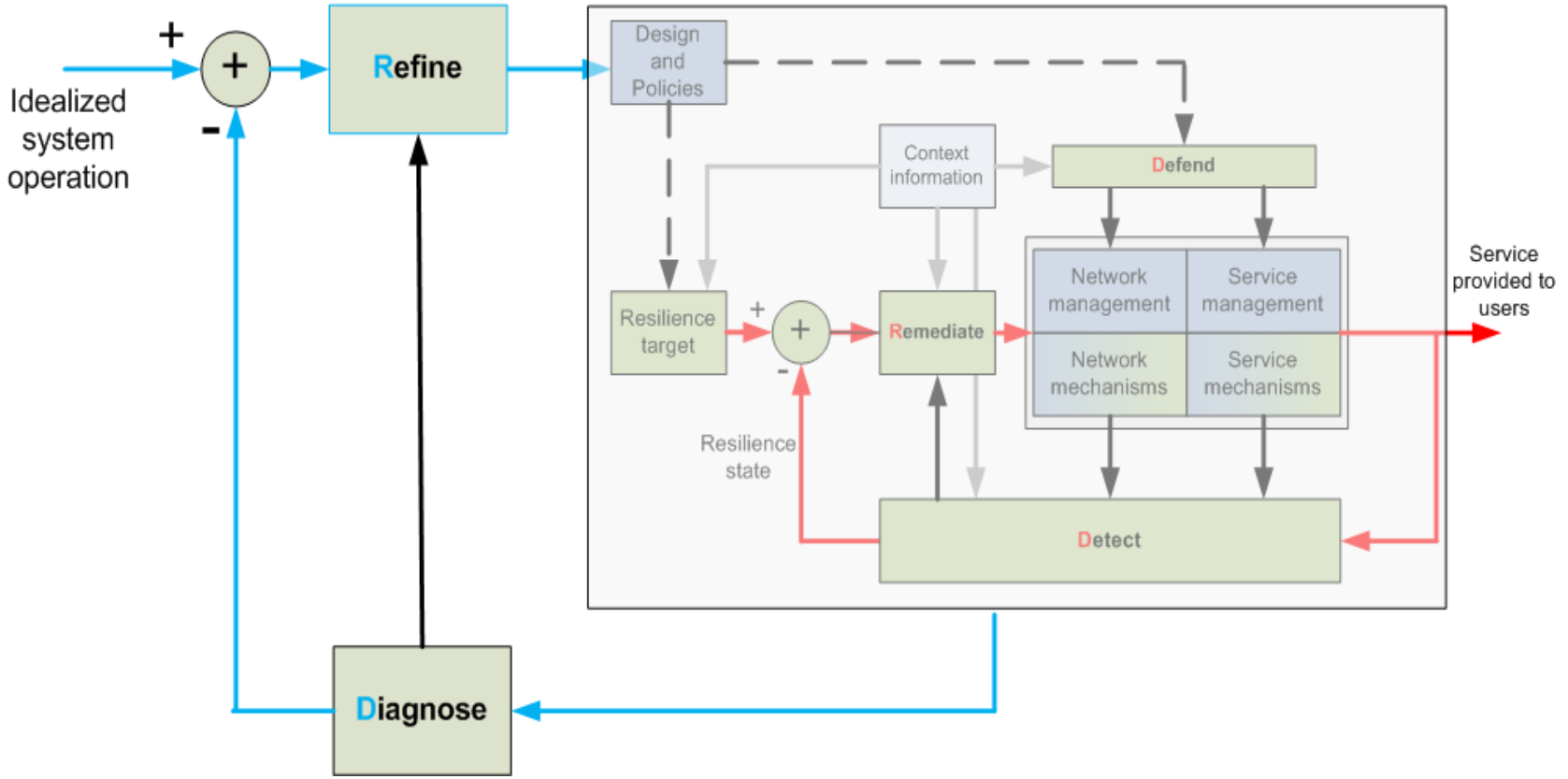


Note: Centralized view of a complex distributed system

Recovery is the desired effect of this feedback loop. Recovery is achieved if the error signal is == 0, i.e. When the measured resilience state is equal to the reference set by the policies

LANCASTER UNIVERSITY InfoLab21

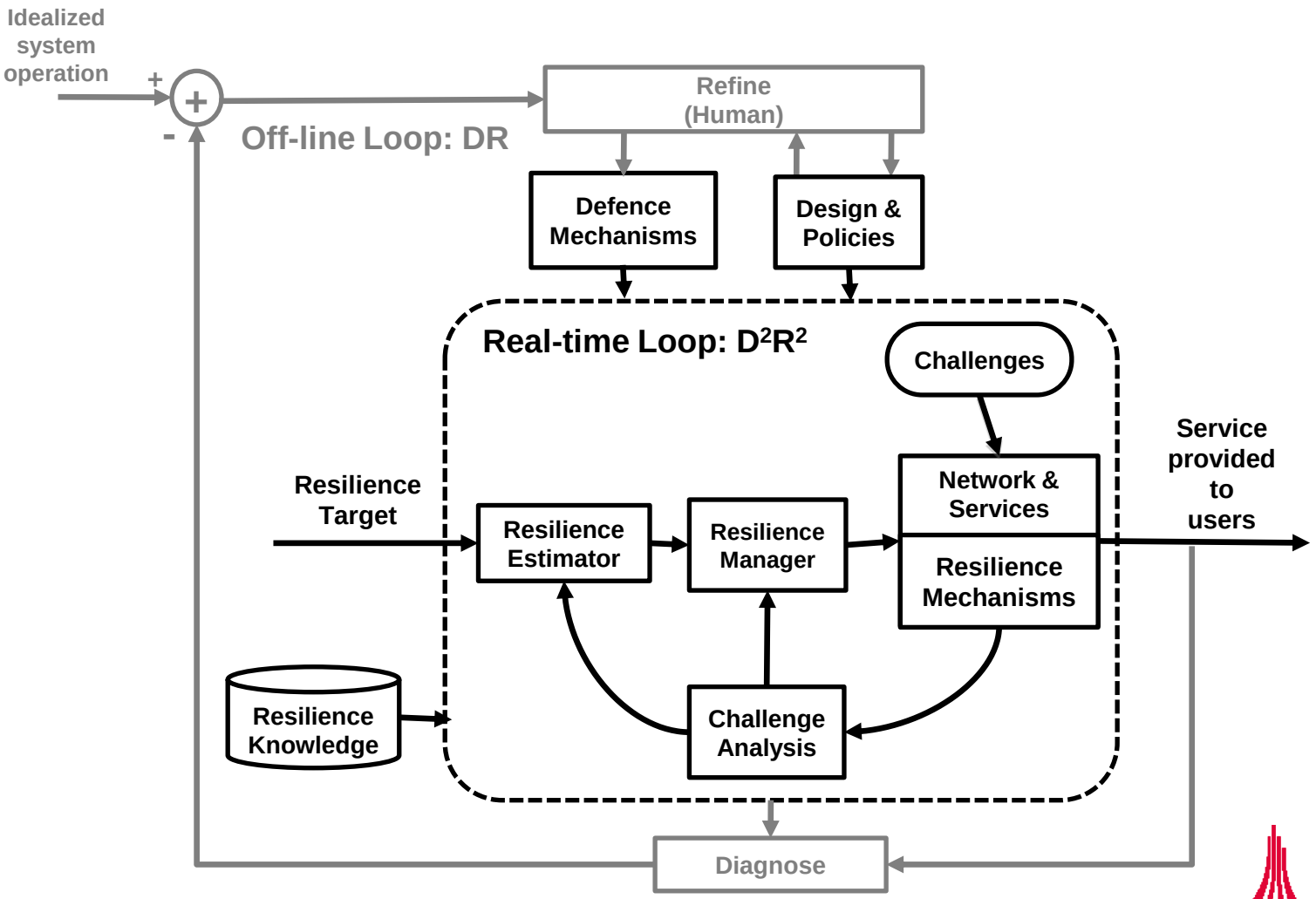
System enhancement: +DR



- Outer feedback loop
- long-term, slow reaction
- Driven by politics or market forces
- humans in the loop : re-design, policy change

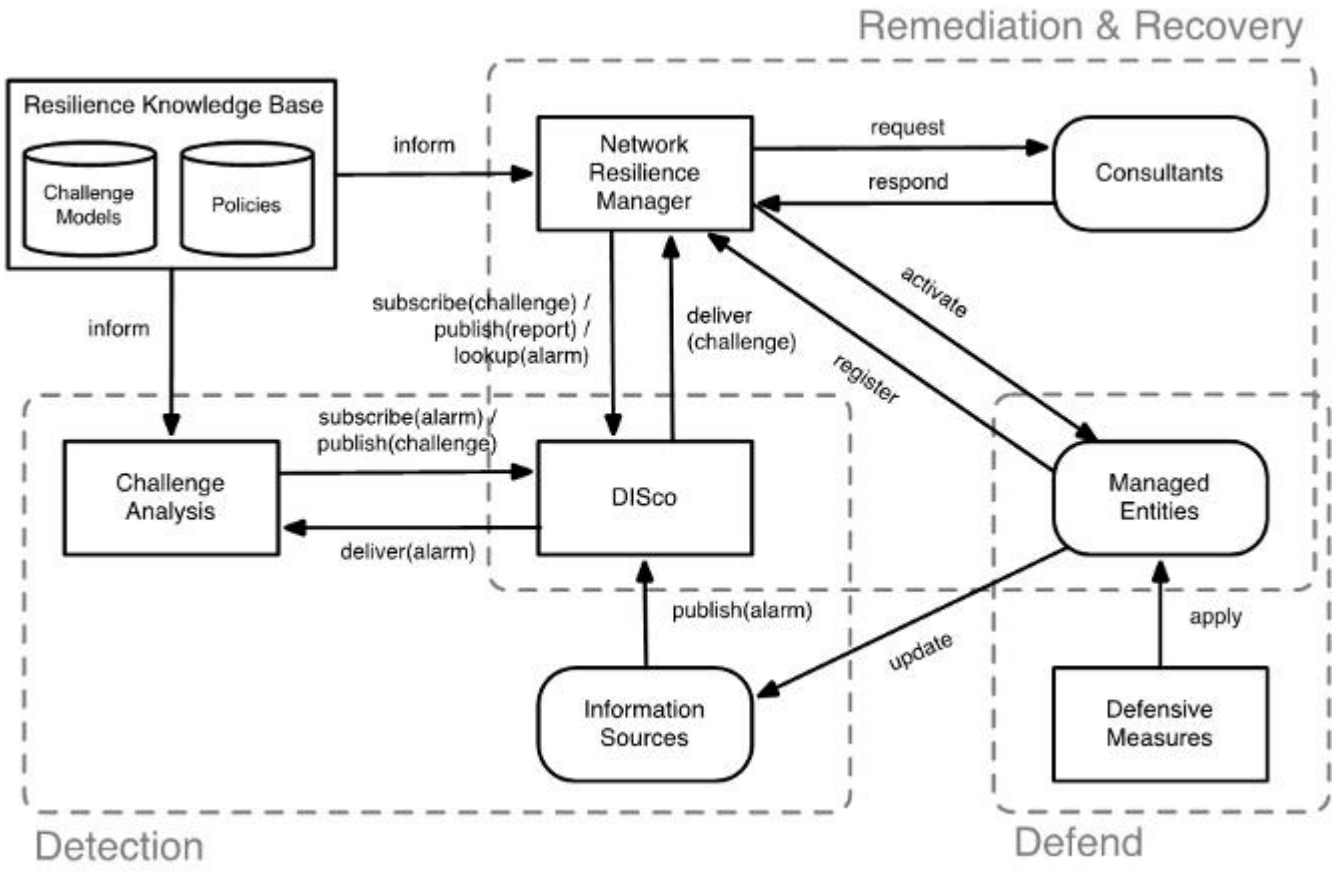
LANCASTER UNIVERSITY InfoLab21

System implementation view



LANCASTER UNIVERSITY InfoLab21

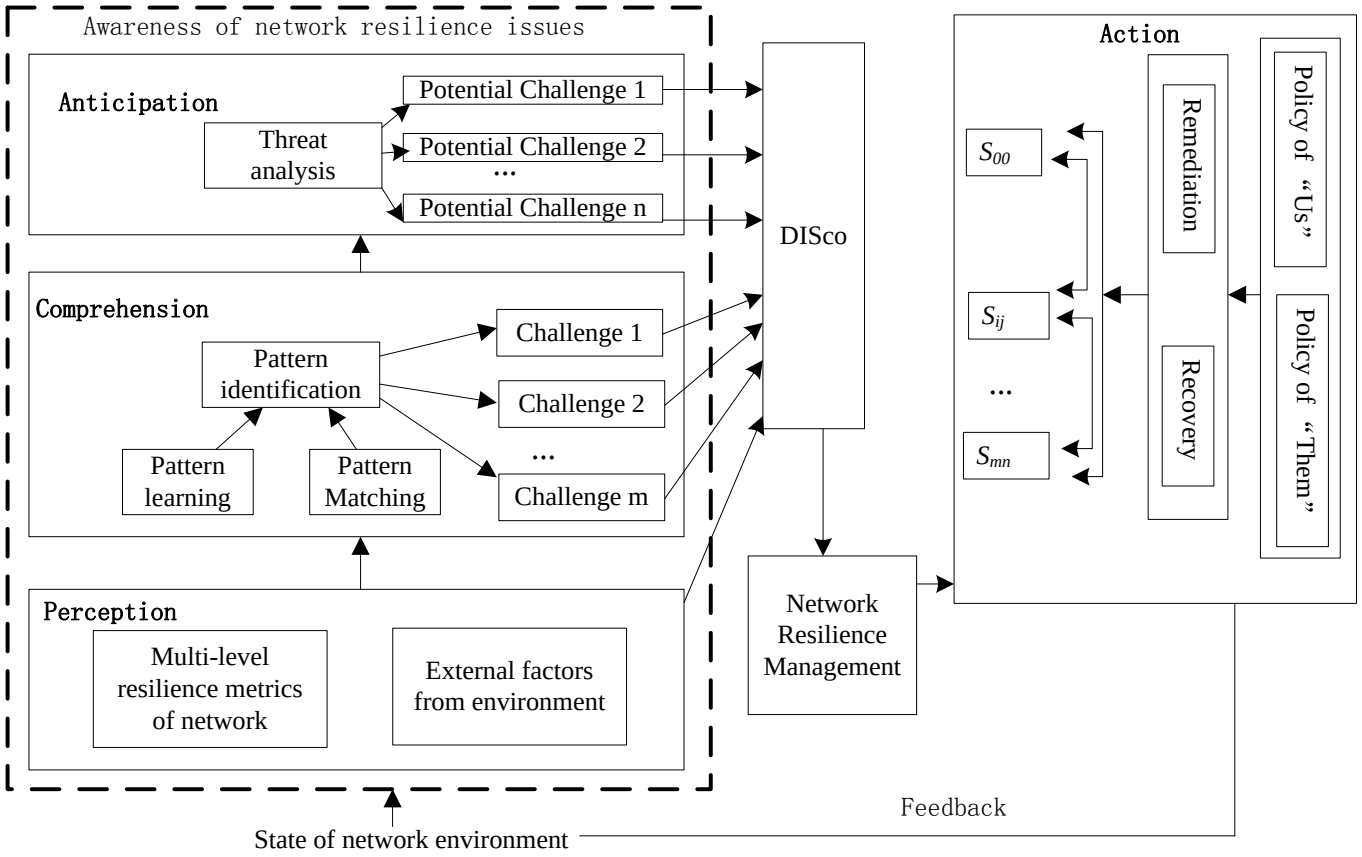
Resilience management architecture



DISco: see Sylvain Martin et al, “DISco: a Distributed Information Store for Network Challenges and their Outcome” (DANMS 2012)

LANCASTER UNIVERSITY InfoLab21

Resilience management via situational awareness



From: "Situational Awareness for Improving Network Resilience Management ", by Mixia Liu et al (ISPEC 2013, LNCS 7863)

LANCASTER UNIVERSITY InfoLab21

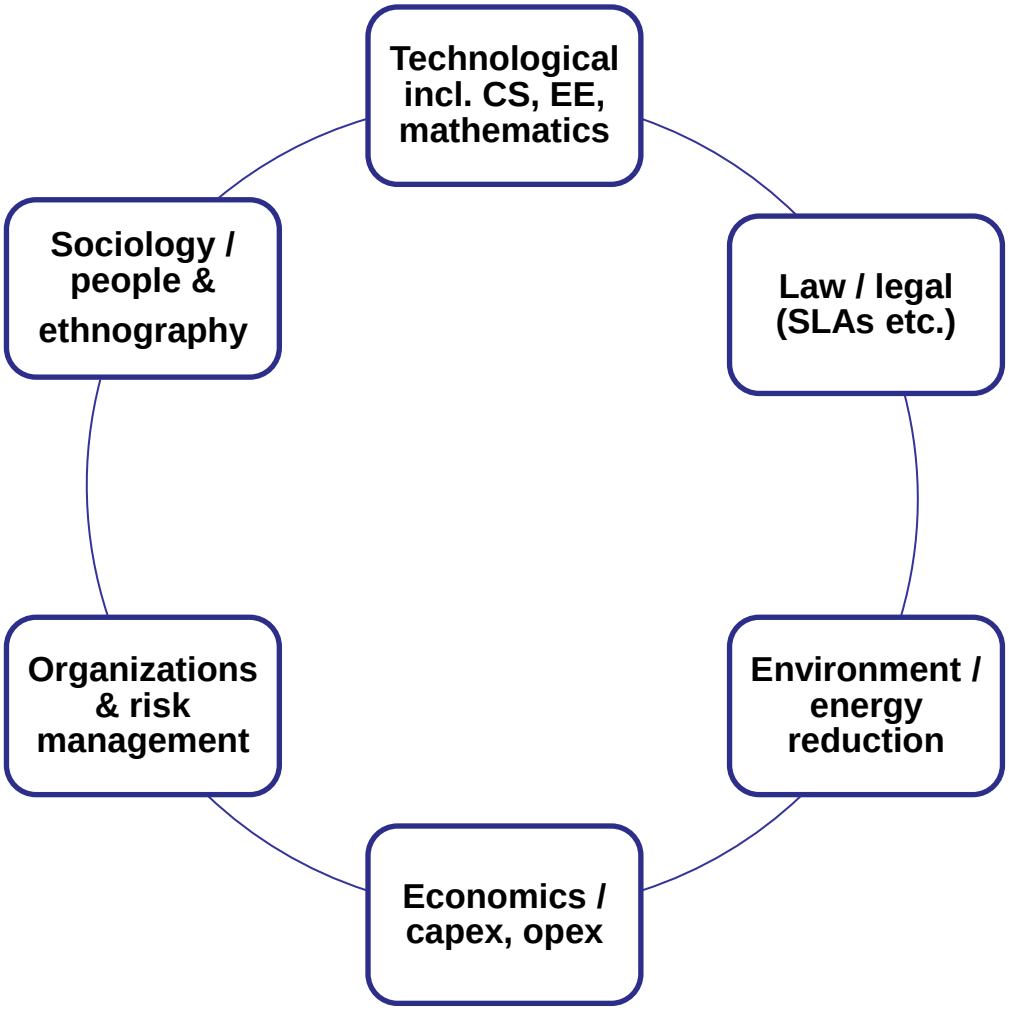
What we have learned (1)

- Our D^2R^2+DR framework is a good basis for resilience research, even though we have not fully investigated the outer loop
- Choosing the right metrics is key to appropriate specifications, measurements, and mechanisms selection to achieve resilience
- Several aspects of resilience remain to be further investigated, including the feasibility of autonomous operation (no human in the (inner) loop …)
- Additional resilience themes have been identified, and should be studied, including resilience classes and situational awareness / projection

What we have learned (2)

- Many organizations still need to be persuaded to make them better appreciate the importance of resilience (and security)
- The relationship between resilience and security needs to be further elaborated, e.g. in the network management area
- We should generalize from communication networks to Critical Infrastructure Protection, including utilities and industrial control systems
- Several disciplinary ‘dimensions’ need to be involved in the development of resilient future networks and systems …

Dimensions/disciplines of resilience



LANCASTER UNIVERSITY InfoLab21

A multi-disciplinary approach

- So, how can we build effective resilience management into the critical infrastructure of Internet networks and services
- We need to design and build a technical sub-system, of course (using our resilience formula / strategy, or elements from it)
- But we also need to understand its implications – for both organizational and human boundaries:
    - Organizational, legal (risk assessment; SLAs, etc.)
    - And ethnography (human in the loop, or not; HCI)
- And other issues including cost-effectiveness and energy use
- It should become routine to study and solve such a problem using the right mix of disciplines
- Internet Science (EU Network of Excellence project) aims towards this ‘normal practice’

A resilience research proposal

- Serene = ‘Secure and resilient networks’
  - Ensuring the compliance of a secure and resilient Future Internet, from specification to operation
- Certification and conformance testing
  - The use of appropriate testbeds
- Include sensor networks and context gathering
  - The use of complex event processing
- Research partners with access to networks/data
  - Network operators, service providers, …
- ENISA have expressed strong interest in the work
  - Critical Infrastructure Protection (CIP) and Resilience Unit
- Looking at EU Horizon 2020 calls, open from Dec 2013
  - Future Internet, Secure Societies/CIP /Resilience Indicator

Further resilience research topics

- Cloud networks and systems
  - Cloud security architecture/management
  - Assessing malware in virtualized systems
  - Risk assessment/management for cloud systems
  - Anomaly detection/remediation methods for cloud
  - Policies/legal approaches/SLAs for specifying/assuring resilience
- Industrial control systems (ICS) and SCADA
  - Hybrid risk assessment for utility networks/systems
    - Ethnography: people and usage aspects
    - Risk management: organizational aspects
  - Security/resilience metrics for ICS/SCADA
  - Functional assurance of ICS/SCADA systems
- Recent/new areas of research
  - Exploring context and situational awareness
  - Botnets/bots detection and remediation in real time
  - Socio-technical approaches to security and resilience
  - Inter-dependent networks; cascading failures problem
  - NFV (Network Functions Virtualization) resilience/security

LANCASTER UNIVERSITY InfoLab21

Projects, references

- ResiliNets (https://wiki.ittc.ku.edu/resilinets/Main_Page)
- ResumeNet (http://www.resumenet.eu/)
- ENISA (http://www.enisa.europa.eu/)
- J.P.G. Sterbenz, D. Hutchison, E.G. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: strategies, principles, and survey of disciplines", Computer Networks, Special Issue on Resilient and Survivable Networks, Vol. 54, No. 8, June 2010, pp. 1245-1265
- P. Smith, D. Hutchison, J.P.G. Sterbenz, M. Schöller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: a systematic approach", IEEE Communications Magazine, Vol. 49, No. 7, 2011, pp. 88-97
- IU-ATC; EINS; SECCRIT; HyRIM (new EU project)

Security and resilience: officially important!

The White House, Office of the Press Secretary, October 31, 2013

Presidential Proclamation -- Critical Infrastructure Security and Resilience Month, 2013

"We must continue to strengthen our resilience to threats from all hazards including terrorism and natural disasters, as well as cyber attacks. We must ensure that the Federal Government works with all critical infrastructure partners, including owners and operators, to share information effectively while jointly collaborating before, during, and after an incident. This includes working with infrastructure sectors to harden their assets against extreme weather and other impacts of climate change."

"I, BARACK OBAMA, President of the United States of America, …, do hereby proclaim November 2013 as Critical Infrastructure Security and Resilience Month."