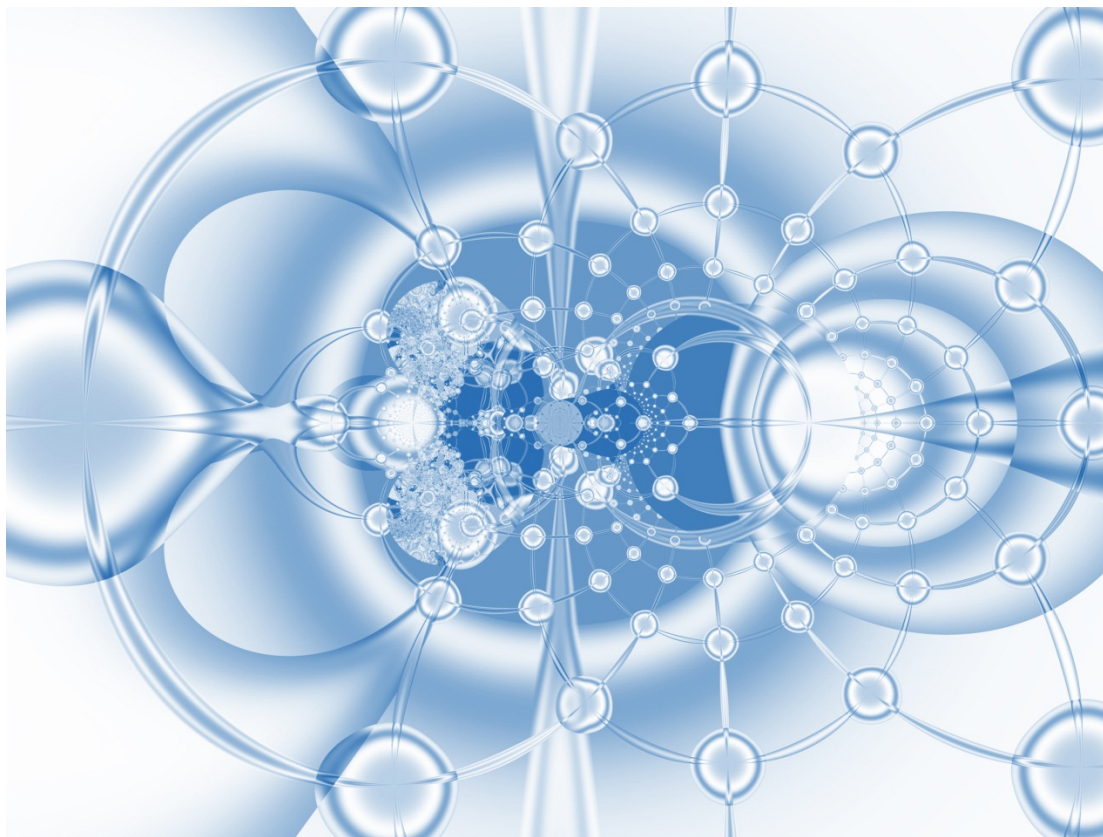


Inter-X: Resilience of the Internet Interconnection Ecosystem



- Introduction to the Study
- Structure of the Report
- Principal Issues and Causes for Concern
- Recommendations

Study url:

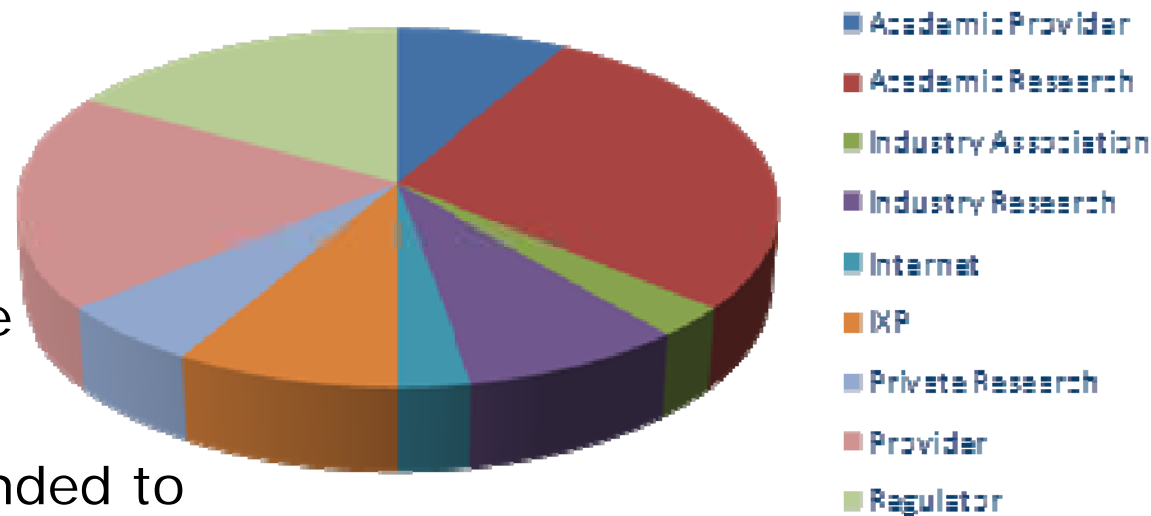
<http://www.enisa.europa.eu/act/res/other-areas/inter-x>

Introduction to the Study

- The resilience of the Internet is important.
- The Internet Interconnection Ecosystem is a key component.
- Objectives:
 - survey the current state of the art:
 - what the ecosystem is
 - what may affect its resilience
 - whether or how that resilience may be assessed (or even verified)
 - where possible, make recommendations for:
 - further work
 - action to improve resilience
 - other research

Form of the Study

- Desktop Study
 - literature review
 - other resources
 - domain expertise/experience
- Consultation
 - questionnaire responded to by many domain experts
 - follow-up questions
 - detailed analysis of the results
- Analysis and Report



Structure of the Report

- Part I
 - Executive Summary
 - Summary of Issues
 - basis for recommendations
 - Recommendations
 - Part II – State of the Art Review
 - identifying and explaining the issues
 - Part III – Report on the Consultation
 - summary and analysis of response
 - Annexes
 - Bibliography
 - Analysis of Major Transit Providers' Financial Statements
- Summary Report
31 Pages
- Full Report
239 Pages

Principal Issues

- Nature / Aspects of Resilience
- Measuring and Assessing Resilience
- Complexity of the Ecosystem
- Routing vs Traffic
- Limitations
- Scale
- Availability of Capacity is Key
- Insecurity
- Common Good
- Lack of Information

Issues: Aspects of Resilience

- Robustness: reduce the effect of events
 - defence: protecting the system so that events have less effect on it.
- Redundancy: cope with the impact
 - prepared response: provision spare capacity and maintain the ability to bring that into service.
- Disaster Recovery:
 - ad hoc response: when an event overwhelms the system's defences and prepared response, that is "major" (a "disaster" of some magnitude).
 - Which may require:
 - temporary measures to maintain "important" services.
 - temporary redeployment of remaining capacity.
 - long term repair and restoration.

Issues: Measuring Resilience

- To measure resilience, need to measure:
 - what effect a given event had (how robust the system was)
 - what impact that had on service levels
 - how long it took to recover to acceptable service levels
 - how long it took to fully restore the system

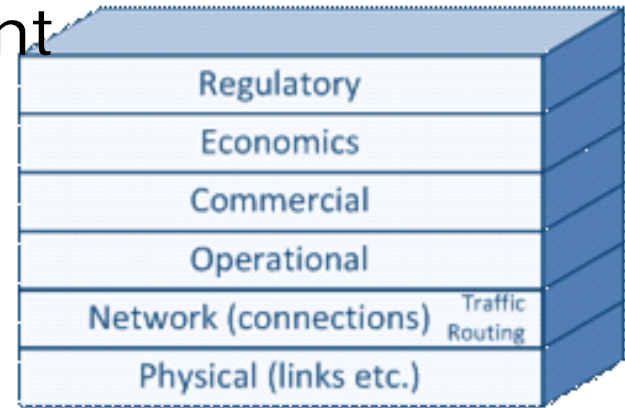
Assuming all these things can be measured (a big assumption), then it would be possible, after the event, to measure how resilient a system was.

- Might also wish to place a value on a given level of resilience, since it comes at some cost!

<http://www.enisa.europa.eu/act/res/other-areas/metrics>

Issues: Complexity of the Ecosystem

- Many complex layers, interdependent
- Physical:
 - electrical power, undersea cables, fire, flood and pestilence.
- Network:
 - re-routes to adjust to failures; but routing itself can fail
 - needs the capacity to carry traffic, and spare capacity to cope in the event of failures
- Operational:
 - monitoring to detect problems and action to mitigate/fix
- Commercial:
 - motivation for any resilience assurance/improvement
- Economics & Regulatory
 - context in which networks operate



Issues: Routing vs Traffic

- Internet Routing – Global Reachability
 - fundamental objective: maintain ability to reach any part of the Internet from every other part of the Internet.
 - achieved by self organising system, working at commercial, operational, network and physical layers.
 - depends on capabilities of BGP, and affected by its limitations.
- Internet Traffic – Capacity and Congestion
 - for reachability to be useful, routes must be able to carry the required traffic.
 - achieved by provision of sufficient capacity.
 - depends on commercial motivation to provide capacity and operational means to detect and mitigate congestion.

Issues: Limitations

- BGP understands routes, not traffic
 - the routing system responds to events by restoring reachability, but has no understanding of traffic and capacity.
 - other, operational, systems must respond to congestion.
- BGP provides little ability to control traffic beyond an AS's borders.
- BGP hides information
 - where it has more than one route for a given destination, each and every BGP router must select one, and will only pass on the one it selects – hiding all the alternatives.
- Each BGP Router makes its own selection
 - an AS has limited understanding of why traffic flows where it does.

Issues: Insecurity

- BGP is “insecure”
 - the routing information carried by BGP cannot be verified, so it is possible for the ecosystem to be disrupted by the accidental or deliberate introduction of invalid routes.
 - The proposed RPKI system is designed to ensure that an AS only announces addresses it is entitled to announce.
 - the proposed BGPSEC extensions to BGP are designed to ensure that the entire AS Path is valid.

- Numbers of ASes, Routes, Routers, Connections, etc.
 - combination and permutation of ~37,000 ASes, ~350,000 route prefixes, etc. – exacerbates the limitations.
- Enormous variation in scale of actors
 - small number of large transit providers and large CDNs, large number of small networks.
- Concentrations of infrastructure
 - clusters of sites and AS-AS links, under-sea cables, etc.
- Literally Global vs local events
 - most physical events are a “little local difficulty”
 - how to assess impact of an event on the global system, and hence the resilience of the system?
 - How about ‘many’ little local events?

Issues: Lack of Information

- There is no NOC for the Internet Interconnection Ecosystem
- There is little to no information available about the working of the system:
 - no map of connections between ASes (could solve)
 - no map of the available routes across the system
 - no map of the traffic flowing across the system
 - no map of the infrastructure on which this all depends
- Without this information it is impossible to say
 - how the system performs when everything is working, or
 - how it copes when things go wrong
 - let alone assess how it might work if things went badly wrong.

Issues: Common Good

- The interconnection ecosystem is a Common Good
 - it is in everybody's interests that the system is resilient
 - it is in no individual network's interest to spend money to help make the system resilient – a free ride is cheaper

Regulation?

- Regulation is viewed with apprehension by the Internet community
 - studies like this are seen as stalking horses for regulatory interference, which is generally thought likely to be harmful
 - the effectiveness of the system to date is seen as evidence of the benefits of an absence of regulation
- The lack of information hampers everyone, including Regulators
 - evidence based regulation requires an understanding of the system, and information about how well it works

Recommendations

1. Incident investigation (by an independent body)
2. Data collection and network performance measurement
3. Research into network performance & resilience metrics
4. Develop & deploy secure inter-domain routing
5. Research into AS (i.e. ISP) incentives
6. Promotion of Good Practices on resilient interconnections
7. Independently test equipment & protocols
8. Regular cyber exercises on Internet interconnection
9. Contingency plans for possible transit market failure
10. Traffic prioritisation / traffic engineering may be needed in disasters, pre-plan
11. Greater transparency – Towards a resilience certification scheme

Questions?



<http://www.enisa.europa.eu/act/res/other-areas/inter-x>