Meeting minutes of the 1st Workshop on Resilience Metrics

December 1st, 2010
Brussels

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Acknowledgments:

ENISA would like to express its gratitude to the stakeholders that provided input to the survey. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

Contact details

For more information about this document, please contact:

Dr. Panagiotis Trimintzios

resilience@enisa.europa.eu

Internet: http://www.enisa.europa.eu/act/res

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Table of Contents

1 AGENDA 5

2 WELCOME AND INTRODUCTION (E. OUZOUNIS) 9

3 EUROPEAN COMMISSION'S POLICY RELATED WORK (V. ANDRIANAVALY) 10

3.1 PRESENTATION SUMMARY 10

3.2 QUESTIONS 10

4 THE ENISA METRICS PROJECT (P. TRIMINTZIOS) 12

4.1 PRESENTATION SUMMARY 12

4.2 QUESTIONS 12

5 RESILIENCE METRICS (R. VON ROESSING) 14

5.1 PRESENTATION SUMMARY 14

5.2 QUESTIONS 14

6 RESILIENCE METRICS IN CONTEXT OF SURVIVABILITY MECHANISMS IN COMMUNICATIONS NETWORKS (P. CHOLDA) 15

6.1 PRESENTATION SUMMARY 15

6.2 QUESTIONS 15

7 MULTI-DIMENSIONAL ASSESSMENT OF NETWORK RESILIENCE (C. DOERR) 16

7.1 PRESENTATION SUMMARY 16

8 RESILIENCE METRICS IN FINNISH REGULATION (H. KIVEKÄS) 17

8.1 PRESENTATION SUMMARY 17

8.2 QUESTIONS 17

9 METRICS USED BY .SE (ANNE-MARIE EKLUND) 19

9.1 PRESENTATION SUMMARY 19

9.2 QUESTIONS 19

10 NETWORK RESILIENCE AND THE LINK TO QUALITY OF SERVICE (F. ROIJERS) 20

10.1 PRESENTATION SUMMARY 20

10.2 QUESTIONS 20

11 PANEL DISCUSSION 22

11.1 OVERVIEW OF MAIN ISSUES 22

11.2 THE PRESENTED INCIDENT-BASED TAXONOMY OF RESILIENCE METRICS 23
11.3 IS SECURITY A PART OF RESILIENCE? 23
11.4 MOST IMPORTANT ISSUE WHEN IT COMES TO ASSESSMENT OF NETWORK RESILIENCE WITHIN AN ORGANISATION / AT A SECTOR-WIDE LEVEL 24
11.5 COULD ADDITIONAL STANDARDISATION OR REGULATORY EFFORTS IN THE AREA HELP? 24
11.6 SUMMARY OF THE DISCUSSION POINTS 25

12 CONCLUSION AND WRAP UP (P. TRIMINTZIOS) 26

Agenda

Within ENISA's program on Measurement Frameworks and Metrics for Resilient Networks and Services, ENISA has conducted the 1st workshop on Resilience Metrics with its stakeholders.

During the workshop, two draft reports from ENISA were presented to the stakeholders for feedback. In addition, a number of speakers presented on the topic and the day concluded with a panel discussion.

The agenda of the workshop was:

Welcome Introduction to ENISA's Resilience Thematic Program	Evangelos Ouzounis Resilience and CIIP Program ENISA
European Commission's policy related work	Valerie Andrianavaly DG Information Society & Media – Unit A3 European Commission
The ENISA Metrics project ▪ Introduction the Resilience Metrics Project ▪ Objectives of the workshop ▪ Progress and findings ▪ Presentation of the challenges and recommendations document ▪ Presentation of the technical report Open discussion	Panagiotis Trimintzios Resilience and CIIP Program ENISA
Resilience metrics	Rolf von Roessing ISACA
Resilience metrics in context of survivability mechanisms in communications networks (Quality of Resilience (QoR)	Pjotr Cholda AGH University of Science and Technology Poland
Multi-dimensional assessment of network resilience	Christian Doerr ResumeNet project

	TU Delft
Resilience metric in Finnish regulation	Heidi Kivekäs FICORA
Metrics used by .SE (TLD operator for .se)	Anne-Marie Eklund .SE
Network resilience and the link to Quality of Service	Frank Roijers TNO
Panel discussion	**Panel:** ▪ Andrew Powell(CPNI) ▪ Pierre Dominique Lassard (Orange FT) ▪ Robert Kooij (TNO) ▪ Rolf von Rössing (ISACA) **Moderator:** Panagiotis Trimintzios Resilience and CIIP Program ENISA
Conclusion and wrap-up	Panagiotis Trimintzios Resilience and CIIP Program ENISA

Summary of the feedback received

The table below represents a summary of the feedback received on the study of ENISA in the field of resilience metrics:

Summary of the feedback received during workshop
Design-based metrics require case-studies to make it clearer.
Topology metrics (i.e. number of cuts to separate one node from the rest) could be included.
Network services are very hard to produce resilience metrics for, but they could be separated into session-based (synchronous) and packet-based (asynchoronous) protocols, along with a couple of examples (VoIP, web, e-mail). Aggregation of the OSI layers is another possibility.
Business continuity to be taken into account – this feeds the resilience requirements.
Report is very IT-oriented: Risk management should be included. Risk appetite determines the level of resilience that is required: Some risks can be accepted, others must be measured. Risk likelihood and impact of service failure must be taken into account.
Resilience is about balancing the cost of the network versus the network service (and associated resilience) offered.
Clarify the difference between network resilience versus network service resilience.
Resilience definition: "Acceptable" can mean acceptable according to a service level agreement or to society.
Socio-technical resilience as a metrics taxonomy domain (for example: Continuity in an IT Operations team in case of illness)
Acceptable thresholds as an absolute value are unlikely
Metrics should be auditable and should have the ability to be expressed in pass/fail.
Impact metrics should be defined. Among others, this could include geographical impact, number of customers affected, ...

Network resilience is not the goal but should serve the Quality of Service. No consensus existed on this statement.
Lack of information on best practices is considered to be a main issue
Lessons from other industries such as gas, electricity, ... can be drawn on critical infrastructure
Resilience is not a binary concept. It is rather a “resilience degree”.
Discussion focuses on fail-safe and preventive approach, need for continuous improvement
The classification between incidents and events beforehand is not always feasible. It depends on how the event evolves and the impact it has on the different systems.
Resilience and security: Each one can be seen as part of the other or as two different concepts. No consensus exists.
Resilience should reflect to whom it refers to.
Standardization will help to make data comparable and available in common formats

Welcome and introduction (E. Ouzounis)

- The ENISA Resilience and CIIP programme started beginning 2008 – end of third year now. It implements, among others, EU Commission CIIP Action Plan. Its focal points are:
    - Policies
    - Technology
    - Provider's measures
    - Good practice guide on info sharing, incident reporting, …
- The programme delivered the first Pan-European exercise on Cyber Security:
    - Testing the abilities of the Member States to work together
    - 22 active players, 8 observers
    - There is clear interest on how this will evolve
- The programme also facilitates the implementation of Article 13a where ENISA supports the interaction of the Member States, assists in the stock taking, and helps the Member States develop a common, harmonised approach in the implementation of the Article 13a.
- Metrics is an important and brand-new area, especially with regards to security.
    - There is a need for an integrated, systematic approach that covers corporate, sectoral, national and even pan-European levels.
    - This is a first, exploratory draft work – the challenges and problems need to be further analysed.
- The level of abstraction and detail for metrics is still an open point for discussion
- The goal of the workshop is to validate the findings of the study and come up with strategic recommendations: These can be used by providers, regulators and potentially on a national or pan-European level.

European Commission's policy related work (V. Andrianavaly)

Presentation summary

- Presentation on the 3 main policy initiatives on Network & Information Security and CIIP of the Commission:
    - Digital Agenda for Europe
        - COM(2010) 245
        - Aim is to provide benefits to society & economy by accelerating the uptake of digital technologies by every EU citizen
        - The seven priority areas for action of the Digital Agenda were briefly introduced, of which one is online trust & security
            - Low trust = low use
            - Goal is to protect the integrity of the information systems but also to improve coordination at EU level for fighting cybercrime (the latter has been the responsibility of EU Homeland Security until now)
            - Cooperation with the key actors: ENISA, CERT's and Cybercrime centre
    - CIIP Action plan
        - COM(2009) 149
        - High level aims of the CIIP action plan:
            - Protect Europe from large scale cyber attacks & disruptions (both from malicious attackers as well as from physical disasters)
            - Promote security & resilience culture (first line of defence) & strategy
            - Tackle cyber attacks & disruptions from a systemic approach
    - Proposal to modernize ENISA (adopted in September 2010)
        - COM(2010) 521
        - Mandate ENISA was until 2012
        - Objectives
            - Become more involved in EP3R
            - Re-enforce capabilities and build on what has been done so far (resources should increase progressively)
            - Triple play:
                - **Knowing better**: Collect, analyse & disseminate NIS data
                - **Working better**: Provide assistance to Member States (cross border issues, detection & response capability)
                - **Cooperate better** between the different stakeholders

Questions

- All problems are global and it seems that the EU is trying to solve them by themselves. Shouldn't there be more international cooperation?

- The last pillar of the action plan is aimed for international cooperation
- In 2009, the global dimension was identified – but the project needs to start somewhere. They started on the long-term strategy for the stability of the Internet.
- In the first phase of the project, focus will be placed on working within the context of the European Forum for Member States on long-term strategies for the Internet. Afterwards, the project will bring the discussion to the global level. One key partner in these discussions will be the US.
- Workgroup with the US was established 2 weeks ago. Following work areas were defined:
  - Stability of the Internet
  - Awareness raising
  - Cyber Security exercise

The ENISA Metrics project (P. Trimintzios)

Presentation summary

- Concerning the ENISA study performed:
    - Motivation
        - Resilience of networks and Critical Infrastructure protection: These topics have been key to many recent policy initiatives.
        - A number of initiatives to assess policies of resilience started within ENISA (metrics and measurements are key to assessment).
        - There was a clear need for work in this area: not that many existing frameworks were identified (certainly no globally acceptable or used policies) and those found were not considered standard practices. Different organisations use different sets of baseline metrics and frameworks. Metrics are difficult to combine/aggregate. Difficult to use for high-level assessment.
    - Objectives
        - Collect information on existing practices and metrics with key experts and stakeholders.
        - Perform a qualitative analysis of input received.
        - Deliver a final report with the recommendations and a list of good practices.
    - Progress
        - Challenges & recommendations report:
            - Input from experts from various sectors
            - **Status: Final draft**
        - Technical report
            - First attempt to a unified view on taxonomy to be able to speak the same language. The baseline metrics were collected from various works out there (first attempt towards full attempt)
            - Network resilience is still not well defined – different meanings are obstacles to discussions on resilience
            - **Status: Discussion draft** (not yet validated)

Questions

- Design-based metrics:
    - Case studies should be included (using a very simple network layout) to show that the resilience metric is higher in certain types of network layouts than others.
      For example: Ring network vs. a double ring vs. a full-mesh network. Any resilience element/criterion used should consider the network design aspects. On larger scale networks, resilience can be linked to the ability of the network to create super-nodes.
- Business continuity needs to be taken in consideration. Service Level Agreement can define the required level of resilience. Operators may not look at resilient networks but at networks that

provide resilience within a SLA. SLA defines acceptable level of service and then the network resilience is built upon it.

- Industry also looks at domains such as supply chain: Not contained in the report.
- Suggestions:
    - Impression that the report is very IT-oriented. There are a lot more difficulties in making networks resilient. Mobile networks evolve very fast to provide the best service at the lowest service but maybe this could be at the cost of the network's resilience. This domain should also be included in the risks of network resilience.
    - Services can be interpreted in many ways: Lower layers of the OSI models can also be seen as services to higher layers in the OSI model. (e.g. routing provides service to transport, this comes back to the question on service resilience versus network resilience.)
    - Conclusion is that much of the terms are usable in an IT-context as well as the business-context.
- Comment on resilience definition: Acceptable is an academic exercise at the lowest level. At a higher level, we should talk about acceptable to society instead of acceptable to a contract. We should make abstraction to the level of acceptable to society.
    - This requires a lot of discussion.
    - Thresholds are important, either from contracts or from society.
    - At this moment, we are interested to see what needs to be measured (either from contracts or from society)
- The risk management layer is missing: The accepted risk defines what is acceptable
    - Some risks can be accepted, some risks are to be measured
- The domains are very broad. Social-tactical resilience of a network is also important. For example: if 2 individuals from IT operations within an organisation are on holiday, what resilience do you have in your operations? Can this be a domain as well?
    - Metrics for resilience should focus on measuring the problems instead of the causes.
- Thresholds
    - Many stakeholders agree that it is unlikely that a certain value is acceptable at a certain point.
    - Socio-political area (grey area) is not included, it is too binary right now

Resilience metrics (R. von Roessing)

Presentation summary

- Overview on what was done at ISACA on metrics
- Metrics are closely linked to governance, risk & compliance
  - Metrics will filter down into compliance requirements and directives
  - They will be used as guidance for companies
- Security as a significant class of risks has been presented (considered by BMIS – Business Model for Information Security). One of the good ISACA instruments that can support ENISA efforts.
- Current landscape of frameworks was presented
  - COBIT
  - Val IT: Value-based framework to link IT to business value
  - Risk IT: Information risk management framework, including risk response component
  - BMIS: Business Model for Information Security, potentially covering a wider scope than just information security (developed at USC)
  - Mappings to external standards, e.g. ISO 27000 series for security
- Future landscape
  - Merge frameworks into COBIT 5
  - Merge and align Val IT and RiskIT into COBIT 5
  - Align BMIS to COBIT 5
- Opportunities to strengthen resilience thinking and extend to network resilience. ISACA seessee BMIS as one key link with the ENISA work.
- Even if ENISA will develop metrics and guidance, ITIL and CMMI are still needed for the implementation part.
- Outlook:
  - Current positioning of frameworks needs more input from network resilience standpoint
  - Controls, governance, risk management and business-facing content may be helpful in bringing pure network resilience into perspective
  - Metrics are developed as generic items (and for security), but not yet for resilience
  - ITIL, COBIT and their frameworks tend to be regarded as good practice in international IT management – any new thinking on network resilience should take into account prior investments

Questions

- Is business continuity to reach the goals that EU and its Member States want to achieve?
  - No it is not sufficient. Business continuity is one of the instruments that support resilience. They are stepping stones but we need to develop more. Business continuity is like a fire detector: If there is a fire, it can detect it. But when there are 20 fire alarms per month, something is wrong with the model used.
- Has the model been mapped to the Telecom framework in the US?
  - No, it has been mapped to ITIL v3.

Resilience metrics in context of survivability mechanisms in communications networks (P. Cholda)

Presentation summary

- Resilience metrics in context of survivability mechanisms in communications networks (Quality of Resilience - QoR)
  - No security has been included
- Resilience is in relation to the design of fixed network.
  - This is an engineering level approach, not a business level one.
- Fault-resilience metrics
  - Survivability metrics: They present a subjective selection.
  - Grouped in 3 groups:
    - Reliability features
    - Recovery-related features
    - Operation-related features
- How to express metrics:
  - Continuity (example: Mean Time to Failure)
  - Downtime (example: Mean Time to Repair)
  - Availability (example: Steady-state availability)
  - Affected traffic/traffic loss: direct & indirect (traffic related to channels that are lost due to the failure, congestions, ...)
  - Failure coverage: Percentage of recovered traffic
- Survivability mechanisms
  - What to select to provide (assumed) levels of resilience?
  - Classification of recovery methods:
- Relation between metrics and methods: examples
  - Histogram of downtime

Questions

- When comparing the optical vs. the IP layer as shown in the presentation, is the experience of user taken into account?
  - No
- Impact of service: When service is available but not used, impact metrics are not very useful.
  - This is why planned maintenance exists. Resilience metrics should take into account that demand is varying (with regards to impact: impact varies as well)
- Which of the presented metrics are most useful?
  - This is the largest problem, no answers available.
  - Only possible for very low levels in the network – metrics depend on which layer you look at.

Multi-dimensional assessment of network resilience (C. Doerr)

Presentation summary

- Multi-dimensional assessment of network resilience as part of the ResumeNet research project
- Goal: Create infrastructures able to withstand
  - Unintentional misconfiguration (BGP for example)
  - Large scale natural disasters
  - Malicious attacks
  - Unusual operating conditions
- Challenge: Anything that perturbs normal network operation: Random equipment failure, terror attacks, natural disasters, maritime cable accidents, cable duct fires, faulty firmware, software exploits, flash crowds, ... Most obscure case: Milk truck that runs over long point-to-point links every day at noon
- Given a network, how resilient is this?
  - Resilience value R, normalised between 0 and 1
  - Mapping function of traffic, network, topology, ... to the R-value
- Which metrics to use?
  - Depends on context
  - Entire stack between service-level metrics and topological metrics can be used
- Mapping of service to operations
  - Service parameters become operational parameters at the OSI layer above
  - Resilience can be evaluated at any arbitrary layer boundary
- Take-home messages
  - Choosing the right metrics is critical
  - Correlation and dependencies may lead to heavy over/underestimation
  - Metric envelopes can give an intuitive understanding of resilience
    - Envelopes help compare networks and quantify the source of degradations
    - Computational system to evaluate impact of failures
    - Impact analysis may be used for resilience optimization

Resilience metrics in Finnish regulation (H. Kivekäs)

Presentation summary

- Resilience metric in Finnish regulation
- Measuring resilience and security – essential regulations
  - 58/2009M: Quality and universal service of communications network s and services
  - 54/2009M: Priority rating, redundancy, power supply and physical protection
  - 9/2009M: Obligation to notify of violations of information security in public telecommunications
  - They add explanatory notes to every binding obligation and recommendations
- Quality regulation (Regulation 58/2009)
  - Provisions on the performance and quality of the public communications networks
  - Obligations on monitoring and measuring quality, operation and performance
  - Some measurements are continuous, statistical data is collected periodically (e.g. use of capacity of video components for each channel for DVB-T network service and DVB-T network service)
  - Others are only done when necessary; e.g. clarify why there was unsuccessful call set-up
- Measurements serve multiple purposes:
  - Observe situation of their own networks
    - Possibility of faults and lacks downs is reduced
    - Faster recovery
  - FICORA can identify trends and challenges and give better guidance
- Security regulation number 9: Security incidents regulation
  - On security incidents, any violations and threats must also be noticed to FICORA
  - Data is collected and trends are analysed
- Key challenge
  - Keep it simple: A lot of data is collected and used within the organisation. It is challenging to come out with qualitative metrics and find out what FICORA can provide to the operators to work better (how to combine metrics into useful data and find trends)

Questions

- Effort required for telecom operator?
  - Operators provide most information automatically (some manual work involved). In case of big issues, FICORA contacts operators themselves.
- Level of granularity required when reporting security incidents?
  - Smaller issues are reported, such as worms
- How do you implement article 13?
  - Already done with regulation 57 - Failures are classified and different data is collected depending on this. Failures impacting more than 1000 users must be reported and verified against statistics.

- When collecting the data, is the data shared back to the operators?
  - For past years, they have seen that there is a need to give information back
  - Operators want to compare their situation to the total Finnish situation. Yearly statistics (anonymized) are given to the operators.
- Quality of provided information?
  - Very difficult to verify, relationship based on trust (trust that they will tell the truth).

Metrics used by .SE (Anne-Marie Eklund)

Presentation summary

- To measure is to know / If you cannot measure it, you cannot improve
- .SE is running a company is printing money – money is invested in the infrastructure.
- Long term goals:
    - Monitor quality of Internet's infrastructure in Sweden
    - Detect deficiencies
    - Promote positive stability in the Internet infrastructure
- One of the focus areas: health check on Swedish DNS domains
    - Number of tools are developed:
        - Healthcheck: platform to collect and analyse data
        - DNSCheck: Checking a domain's general health
        - MailCheck: Checking different quality-related aspects e-mail setups
        - DNS2db: Used for traffic analysis
        - DNSMon: Monitoring .SE DNS services
        - Bredbandskollen (measuring bandwidth)
    - Reports are showing over 25% of Swedish domains with issues – impacting their availability. .SE would like to reduce this number.
    - Error is defined as something that seriously impact the availability and reachability of a domain.
- Resilience is applicable from different perspectives:
    - Availability
    - Security
    - Safety
- Try to learn from other areas
    - Electric power industry
    - Transport industry (flight, boat, train)

Questions

- It seems like a lot of measurements are on standard compliance
    - Monitoring is essential, they aim for 100% availability (important for customers, reputation).
    - DNS checking is compliance (but a poor DNS leads to a security vulnerability)
    - Difference between compliance and metrics
- If they don't comply, will you unregister their names / lock the domain?
    - They try to push them forward by showing consequences

Network resilience and the link to Quality of Service (F. Roijers)

Presentation summary

- Network resilience is not the goal of the operator. An operator wants to give the SLA-agreed service: Providing connection availability, while satisfying the other metrics as agreed in the SLA
- Availability is provided by the network and processes:
    - Design before deployment: First line of defence by rerouting/backup paths.
        - Need for a method to provide trade-off between risk and costs.
        - Metrics is always used as an average number
            - But customer experience is not the average availability
            - SLA value should be met **every** year
        - Proper calculations lack in general
    - Pro-active prediction of future performance degradations
        - KPI's to assess the effect of architectural, equipment or process changes
        - Many aspects influence the Quality of Service:
            - Architectural choices are never revised in practise (a fair decision for single point of failures during the design phase becomes unacceptable in later years)
            - Technology runs end of life
            - Performance degradation
            - Measurements remains unused by NOC
- Conclusions:
    - Resilience is not the goal but should serve the QoS
    - Resilience can be implemented in the network or in processes for design & network monitoring
    - Direct monitoring of service quality is hardly implemented
        - Mainly focused in resource performance monitoring
        - Customer connection monitoring
    - More KPI's should be used
    - Automated statistical analysis

Questions

- Forecasting issues
    - Be very careful when only looking only at the network (risk of becoming blind to other issues)
    - In Norway, operators monitor weather forecast. In case of bad weather, maintenance crew prepares themselves. Raising the preparedness level in case of challenges: This has nothing to do with the network itself.
- Resilience is not an objective while Quality of Service is an objective.

- This is considered to be a controversial statement.
- ENISA thinks that Quality of Service is part of resilience and that resilience is an objective on its own (in view of the wider policy)

Panel discussion

At the end of the workshop, a panel discussion was held which focused on:

- The main issues with resilience.
- The presented incident-based taxonomy of resilience metrics
- The question whether security is a part of the resilience concept or if they ought to be considered as two separate concepts.
- The most important issues when using resilience metrics to gain intelligence on a sectoral or even pan-European level.
- The question whether additional standardisation and/or regulation efforts could advance the area of resilience metrics?

Overview of main issues

- **Andrew Powell (CPNI):**
    - Large difference between **network resilience and network service resilience** (considered to be a harder problem)
    - When talking about impact, time to recover, MTTF, there is a **probability** attached to it. The whole issue of metrics needs to be seen in the light of **risk management** (likelihood and impact of service failing and how to manage that)?
- **Robert Kooij (TNO):**
    - Resilience is a very difficult issue. Telecom operators mainly want a high quality service – **resilience is not the main objective**.
    - Notion of **smart metrics** is important: Not only average metrics, but also probabilities and statistical distributions should be used as tools
    - **More information on best practices** needed (operations of large telecom operators)
    - Lessons should be drawn from **other industries**: information exchange with gas, electrical, water industry (example: How do they manage critical infrastructure?)
- **Pierre Dominique Lassard (Orange FT):**
    - **Business impact analysis** and BCM could be improved (metrics should be found in that area to precise the impact). Maybe '**impact value'** could be investigated as a metric: geographical aspect, number of people impacted, ... (example: Impact value of terrorist attack)
    - Issue with the incident-based approach presented in the technical report: Telecom operators have hundreds of incidents per day and almost all incidents don't impact the resilience nor the customer. Resilience should be seen in the light of business impact analysis.
    - We spoke about network resilience, not on service resilience. We might need to define a **resilience degree** (resilience is not binary).
    - There is a clear need to consider the customer and also the national/European authorities who will **impose obligations on the resilience level required** from an operator.

- **Rolf von Rössing (ISACA):**
    - Despite the efforts done for identifying metrics, it is not a self-serving purpose. Economics will dictate the question how much resilience is considered to be enough resilience. This is determined by the **risk appetite** business managers might have (who do not think at a technical level). There is a need to bridge the gap between academia, technology and business.
    - When recommending resilience metrics, there will be a **financial question** behind every recommendation.
    - **Fail-safe / preventive approach** is very much in mind during the discussions, while preparedness and managing the network should be addressed in the phases to follow. There should be a **continuous improvement**.
    - Resilience exists under the control of the governance department. This will have an impact on the (preferred) metrics. **Metrics should serve auditability** and should have the ability to be expressed in a pass or fail.

The presented incident-based taxonomy of resilience metrics

- It is probably not good to report everything but the **creation of an automated system** could relieve the effort and increase awareness.
- Metrics can be used as an **early-warning system** to indicate in sub-optimal system conditions
- The **term 'incident' could be confusing**: Incidents are handled by network management teams for several years for hundreds of incidents per day and have nothing to do with resilience. Better terms could be 'crisis', 'big incident', 'disruptive events' or 'significant-impact event' (term used in Article 13).
- Many classifications suggested dividing small events and large incidents. **Systematically classifying events beforehand is not considered to be feasible**: an event of unspecified nature will be an unknown for the first hours.

Is security a part of resilience?

- It depends on the understanding of security:
    - If security is about Confidentiality, Integrity and Availability: As resilience deals with **a lack of availability**, resilience could be called a part of security.
    - Another opinion was that security is the aim to stop people from doing things that alter system behaviour; it can also comprise non-intentional acts. Taken into the broader sense of **Business Continuity Management**, security can be a part of resilience.
    - When looking at the different ways in which a network can fail, both security-related causes exist (e.g. worms) while others can be related to hazards (buggy firmware). They all exist under the **resilience umbrella**.
    - Security plays a major role (e.g. threats in cyberspace) to the resilience and it links to the aspect of quality (available, integer and tightly knit together). As such, security can be considered a part from resilience.
    - **Business Continuity Management** used to be part of risk management. Controlling was first seen as part of accounting. It is inherent to human nature to try to classify the

unknown. Resilience could be seen as sustainability (network's ability to snap back to the original state after an incident). **Resilience will be standing on its own, apart from security.**

- The panel members agreed no consensus exists.

Most important issue when it comes to assessment of network resilience within an organisation / at a sector-wide level

- **Business-level impact** is the most important to assess. The topology and structure of the network as a whole should be taken into account when assessing possible impact.
- While topology is a means to deliver the services, **service resilience** could be much more important (looking at how the customer experiences the service).
- **Degree of resilience**: Resilience should not a binary measure.
- In order to measure sectoral or pan-European resilience levels, enough empirical data (respecting privacy) should be collected to have a good picture of the incidents which happened. The **greatest challenge will be the data gathering** and the ability to tell if the network was indeed down or if the outages were caused by another issue.
- Resilience is not a one-dimensional parameter: **Economics and cost of the service** should be taken into account. Low-cost services can have less resilience (which is accepted by the customer as a trade-off for a lower price for example).
- **Definition of resilience lacks 'whom for?'.** The resilience level required depends on who the customer is. As an example, the emergency call center '112' must guarantee a service level (maximum delay to response). However, for example for personal e-mail, no requirements are set to the service. The 'for whom?' question is in fact equivalent to the impact question.
- **Resilience is not the same as service level measurements**: Resilience is measuring the incident and how we can come back to the normal service level.
- **Concept of resilience is still unclear** when compared to security.
- Information security is very different from network security; resilience on the network is also different from resilience in general. It is important to keep focus and to define the relevant properties.
- Resilience metrics require a model, a scale and a range. Resilience must be **put in a certain context (resilient against what?)**.
- **Resilience cannot be 100%**: What should be considered as optimal resilience?

Could additional standardisation or regulatory efforts in the area help?

- All Member States should share information on their disruptive incidents **– standardization can help to make data comparable** and made available in the proper formats. This can be enforced via regulations.
- Additional standardisation is required: **Definitions** could help (e.g. 'a fully resilient network is defined as', 'a partially resilient network is....'). This is a **prerequisite to regulation**: You can only oblige things that have been defined. As soon as a resilient network can be defined, regulators can enforce resilience in a way that makes sense.

- Regulation can be useful if **based on good practices**. Regulations should not be an exercise in ticking boxes and should not limit commerce. They can ensure a secure and safe way to do secure business and be safe online.
- Regulating right now is not the right approach - first, **tolerance on impact and disruptions should be defined**.
- Even in the DNS world where standards exist, it is difficult to determine what to measure. **Regulations can only happen when we get the definitions right** (networks vs. services). This could be done by documenting case scenarios and a decomposition of definitions.

Summary of the discussion points

- There is a **clear need for definitions of resilience concepts**. Definitions will pave the way towards the **implementation of regulations**.
- In addition to the definition, a distinction should be made between network resilience and network service resilience.
- Resilience should always be related to the **impact of a failure**.
- **Resilience is not a self-serving purpose**: It must be seen as a tool for risk management to assess the service and network risks. Therefore, metrics must be quantifiable and auditable.
- Resilience metrics should include a dimension of **risk management** (the likelihood of failure and the associated impact).
- **Techniques such as statistical distributions and probabilities** are very useful for resilience metrics.
- **Best practices should be shared and documented** (even illustrated with case studies), before regulations or standards could be set. A basis for these best practices could be found in other industries that depend on critical infrastructure (e.g. the utilities sector).
- **Different taxonomies** have been proposed but **no consensus exists** on the categorization of metrics.
- **No consensus exists on the relationship between security and resilience** – they can be subconcepts of each other while it was also suggested that they are two independent concepts.
- Data gathering and analysis is still an obstacle towards measuring resilience. When assessing resilience in a sectoral or pan-European context, standardization can help to make the data comparable and available in proper formats.

Conclusion and Wrap up (P. Trimintzios)

- Wrap-up
- Summary of the objectives of the workshop and their remarks/follow-up actions:
    - **Objective**: Present the draft findings of the ENISA study
        - The draft findings were presented, in the form of a 'Challenges and Recommendations' document, as well as in a 'Technical Report'.
        - No consensus was reached on following questions:
            - Can be the incident-based classification be overall accepted?
            - Which domains should be included in the taxonomy?
            - Is the baseline metrics template adequate?
            - Which impact factors shall we use?
        - The participants **acknowledged the value of the study** but no consensus was reached on how to improve the document.
    - **Objective** Gather feedback from the expert community
        - The different questions after the presentations and the panel discussion provided for very interesting feedback.
        - The participants agreed that **resilience metrics require more research** before the metrics can become a practical tool.
        - There is a strong feeling that **sharing of good practices** can significantly speed up the process of adoption.
    - **Objective** Listen to expert presentations
    - **Objective** Discuss the controversial/open issues, the recommendations and the next steps
        - The panel discussion and presentations provided a comprehensive view on the different open issues.
        - There is consensus that the open issues remain.
        - ENISA's next steps are:
            - To integrate the feedback from the workshop and further discussion with experts
            - To finalise and public the presented reports
            - To follow-up on the recommendations formulated today
            - To support more work on metrics, especially on the identified open issues.
            - Provide input to the Article 13a and data collection work
    - **Objective** Create a community and wider consensus around resilience metrics (probably followed next year by creation of a virtual expert group)
        - This workshop was a first step towards the creation of a community – in the future, more workshops could be organised where a higher level of interactivity is possible.
        - ENISA will keep the stakeholders engaged: revised reports for comments and any further activities in the area will be communicated to them.

enisa
European Network
and Information
Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu