EP3R 2013 – Position Paper

Position Paper of the EP3R Task Forces on Incident Management and Mutual Aid Strategies (TF-MASIM)

FINAL, 1.0, December 2013

ean Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Lionel Dupré, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This Position Paper was prepared and developed by the following Experts:

- Peter Burnett, Quarter House Ltd
- Genseric Cantournet, Telecom Italia
- Manuel Carpio, Telefonica
- Christian Doerr, University Delft
- Olivier Duroyon, Alcatel-Lucent
- Diego Fernandez Vazquez, Isdefe - Ingeniería de Sistemas para la Defensa de España
- Stuart Goldman, The East West Institute
- Bastiaan Goslings, AMS-IX
- Chris Gow, Cisco
- Matthew Holt, Intellium Group
- Jeanette Innes, Independent Consultant
- Richard Krock, Alcatel-Lucent
- Nikolaos Loukeris Vodafone Group
- Sam McLaughlin, Thales Group
- Gerald McQuaid, Vodafone UK
- Michael O'Reirdan, Comcast
- Christian Proschinger, GovCERT Austria
- Karl Rauscher, The East West Institute
- Paul Smith, Austrian Institute of Technology
- David Sutton, Tacit.Tel
- Nikolaos Tsouroulas, Telefonica
- Peter Wallström, Swedish Post and Telecom Agency – PTS

Executive summary

This document summarises the discussions that happened between April and September 2013 in the EP3R Task Force on Incident Management and Mutual Aid Strategies.

The task assigned to this Task Force was to reflect on the potential issues found when a large scale incident (Cyber, Natural Disasters, etc.) affects the Critical Information Infrastructures in a region across one or several borders.

While many aspects can be recovered from without the help of a neighbour country, some actually require external assistance, and therefore cooperation terms can be prepared in advance to plan for those conditions of intervention properly.

Also, the Task Force felt that systematic cooperation on incident preparedness would allow a much faster recovery, particularly for 'black swan' events, i.e. events that have a low probability but generate an extremely large impact.

Some agreements have been established, but they are mostly ad-hoc. The preparedness process could benefit from a higher level of maturity of its cross-border dimension in Europe.

Compared to other continents, Europe still faces significant barriers:

- Cooperation between counterparts in neighbour countries is ad-hoc;
- National Regulations demonstrate several differences;
- Private Sector operates mostly in Silos;
- Mutual Aid Assistance could allow a much shorter Time to Recovery, and a more mature approach to Incident recovery.

The Task Force reflected on three different scenarios and identified a number of gaps.

This Task Force was composed of Public and Private Sector Experts who all contributed their observations in the course of 2013.

The major conclusions are the following:

- A 'Incident Preparedness and Coordination Expert Group' should pave the way to an improved cooperation in the Telecom Sector;
- A RSS-syndication type of platform for sharing Incidents Preparedness procedures, Early Warnings, and Contact details should be designed and used;
- The pan-European environment for Mutual Aid Assistance should be enhanced significantly by removing any relevant regulatory barriers;
- Policies for cross-border traffic prioritisation should be developed and tested.

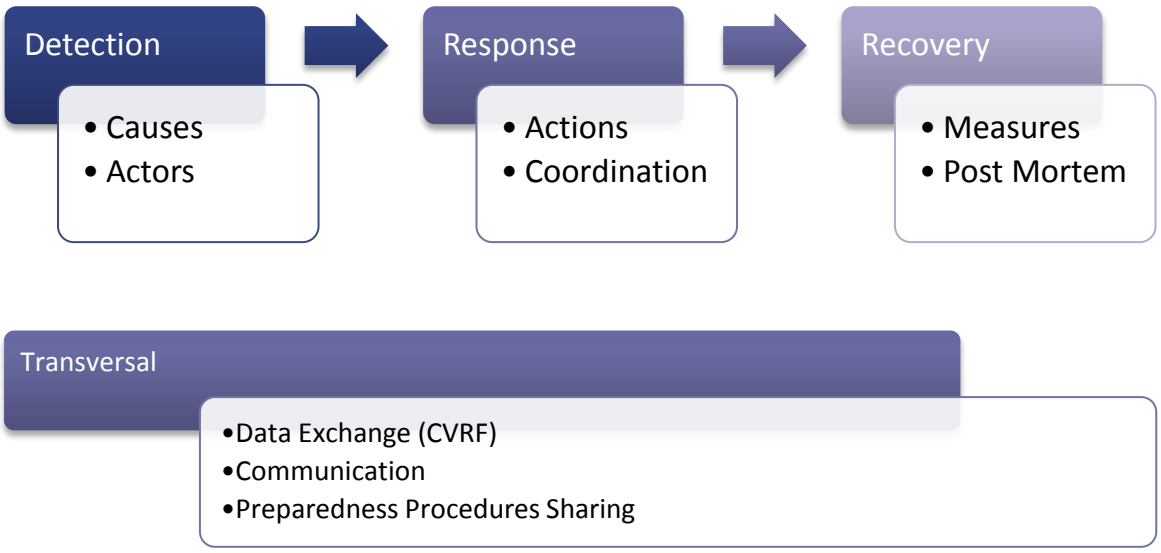
Table of Contents

1 Introduction

In the view of identifying possible gaps and issues in Cross-Border Incident Management in Europe, we have, together with the EP3R Task Forces, imagined 4 different scenarios that we have then tried to reflect upon and draw a number of key conclusions.

Goal

While most of these conclusions might be well known already, this position paper will at least help to inventory them and further support the development of a course of action.



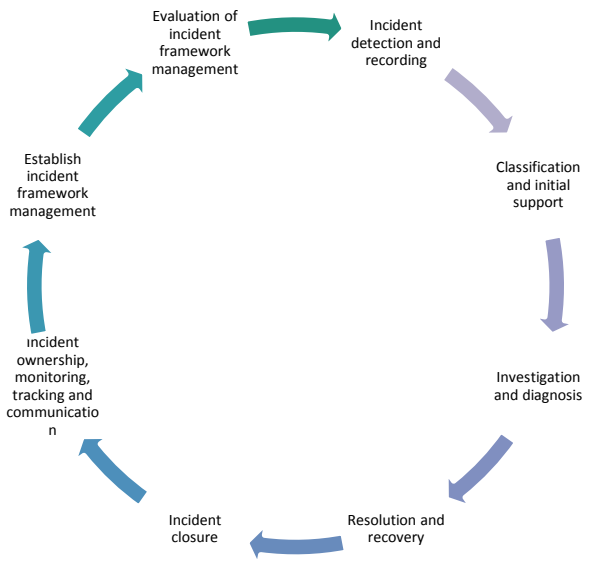
Scope of the Work

The Task Force observed initially that “Incident Management” is a broad concept that encompasses a number of very different activities.

ITIL (v3) terminology defines an incident as an unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident.

ISO 20000 defines an incident (part 1, 2.7) as any event that is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service.

Generally, the process of Incident Management is composed of a number of activities (see figure on the right).



It is generally reported that Incident Management in the ITIL and ISO sense of the term are well managed within each Telecom Operators' boundaries[1], [2], [3], [4]. The issue specific to Europe is indeed cross-border, cross-companies Incident Management.

The figure on the right shows what the Task Force considered, and the parallel can be made to the ISO/IEC 27035-1 (which is still a draft document, to date):

- *Plan and prepare: establish an information security incident management policy, form Incident Response Team etc.*
- *Detection and reporting: someone has to spot and report "events" that might be or turn into incidents;*
- *Assessment and decision: someone must assess the situation to determine whether it is in fact an incident;*
- *Responses: contain, eradicate, recover from and forensically analyse the incident, where appropriate;*
- *Lessons learnt: make systematic improvements to the organisation's management of information security risks as a consequence of incidents experienced.*

Taken individually, these steps make sense at an organisation level. However, when the dimension is cross-organisations, cross borders, the need for a coordination mechanism arises and other compensating controls also need to happen.

As devised in the initial Work Objectives document, the disastrous events, and many incidents are global and cannot be addressed using a silo approach, and cooperation is more efficient when

[1] https://www.ovh.com/fr/espace-presse/cp1028.ovhcom_obtient_la_certification_isoiec_27001_pour_la_fourniture_et_lexploitation_dinfrastructures_dediees_de_cloud_computing

[2] http://news.o2.co.uk/?press-release=telefonica-uk-safe-as-houses-with-iso-27001-achievement

[3] http://www.telecomitalia.com/tit/en/sustainability/our-approach/indexes-ratings/certifications.html

[4] http://www.telekom.com/corporate-responsibility/data-protection/65336

properly planned. Responses also need to be coordinated and the most obvious cases have to be at least foreseen.

In the essence of time and work efficiency, the Task Force has decided to demonstrate by example the issues that must be resolved for quick recovery when the disaster or the incident is global.

The scope for each case Study was limited to "Black Swan" events, rare in likelihood but leading to a disastrous impact.

Target audience

This document addresses concerns that should draw the attention of Telecom Operators, ISPs, IXPs, Datacentre Operators, and most specifically their Decision Makers. CISOs, Business Continuity Managers, Risk Managers are the primary Audience of this report; however the Senior Experts from the Public Sector and Public Decision Makers also should be aware of the high-level recommendations.

Structure of this document

Three case studies were assessed:

- Case Study 1: Natural Disaster involving 3 countries and 5 major Telecom Operators (CII owners)
- Case Study 2: Loss of communication for Health and Finance sector
- Case Study 3: Technologic Implementation causing failure with Domino effect to competitors

The approach was to assess broadly the possible impact, and identify a number of specific measures to support faster recovery.

The ITIL and ISO terminology definitions of Incident management were used as a foundation for the overall discussions[5].

The Task Force proposed to perform the analysis from an empirical viewpoint and therefore requested ENISA to propose 3 Case Studies which could be used as the starting point for the brainstorming sessions of the Task Force.

The process was to determine important lessons learnt by sharing Task Force members' experiences. These lessons learnt were then used to derive key measures.

[5] http://www.iso27001security.com/html/27035.html

The Task Force considered this process as a progressive one, possibly involving several iterations to reach a better level of detail with time and experience.

Although for the purpose of this report, the process only involved a single iteration, the iterative process should be pursued and recommendations could be refined and adapted.

The Task Force used case studies to identify a number of possible black-swan events (which have low probability, and high impact, e.g. 9/11 in the United States).

The initial scope covered the following topics:

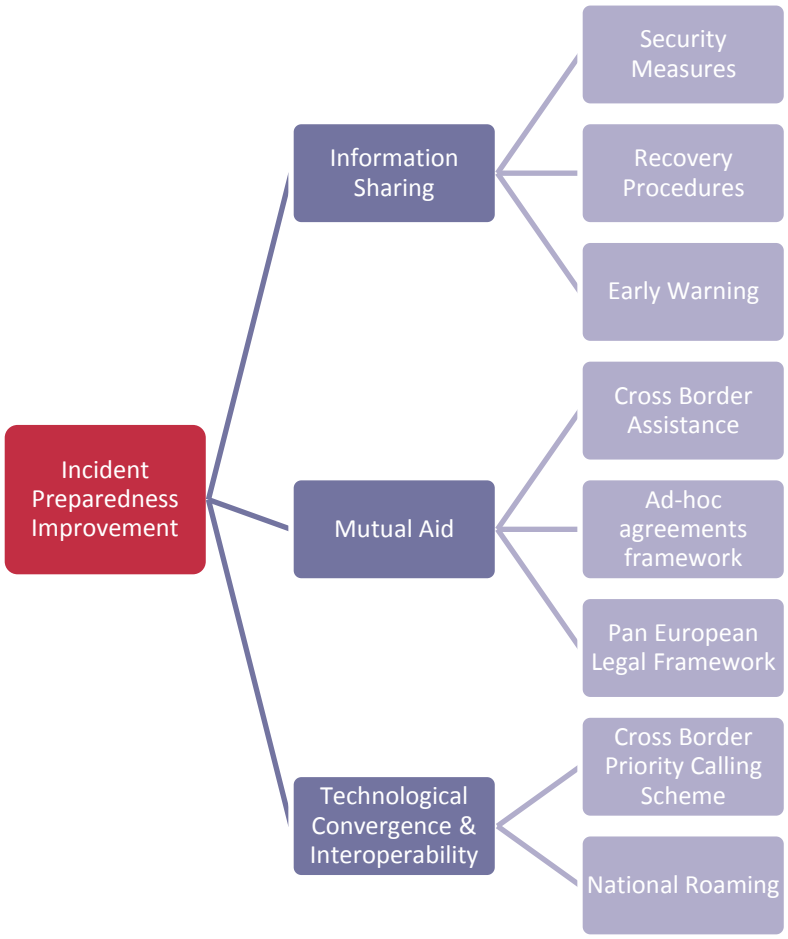
- Natural Disasters;
- Global Power Outage;
- Technological deployment cascaded failure, and chain of events.

These case studies were not meant to be limitative, and pave the way to draw conclusions in other areas. The logic observed for large-scale incident response might reasonably be similar in most situations, and therefore, this report makes recommendations that are generic enough to allow use in a variety of circumstances.

Three main areas are Operational, Technical and Strategic:

- Information Sharing
- Mutual Aid
- Technology Convergence & Interoperability

In each domain, a number of measures were derived and are possible future recommendations in this area, since they are focused and close-ended.



2 Case Studies

The following scenarios were analysed by the participants:

- Natural Disaster involving 3 countries and 5 major Telecom Operators (CII owners)
- Power Outage, loss of communication for Health and Finance sector
- Technologic Implementation causing failure with Domino effect to competitors

2.1 Case Study 1: Natural Disaster involving 3 countries and 5 major Telecom Operators (CII owners)

2.1.1 Description

An earthquake in the Alsace plain impacts France, Germany and Switzerland and causes cable cuts, power outages, etc. All power generators are no longer functioning; GSM relays are out of order.

Initial assessment shows that there are many casualties; First Emergency Responders (FERs) rely on dogs to find them in the debris. Some CIIs sites are no longer accessible.

2.1.2 Impact Analysis

A natural disaster such as an earthquake or large forest fire may require that communications continuity is ensured, or restored in the shortest delay.

All Natural Disasters will not present the same characteristics, but from a telecommunications point of view, the depending actions should be very similar, provided that the road access is at least cleared to the damaged area.

The Task Force perceived that communications between the Public and First Emergency Responders (FER) are crucial, but there is also a need for the Public to be able to contact their relatives, or coordinate their evacuation of the accident. Such communications traffic is unlikely however to be routed properly if the Critical Information Infrastructures (CIIs) are damaged or destroyed.

This raises immediately the question of a priority calling scheme to ensure that every call from the accident zone is appropriately routed and reaches its destination. (see recommendation 201304).

A number of gaps were noted:

- For large events, no supra-National coordination mechanism exists; (see recommendation TF-MASIM-201301)
- Procedures are not established a priori along with affected public emergency co-ordination authorities to declare and manage the crisis; (see recommendation TF-MASIM-201301 and 02)
- Congestions will occur due to significant incoming traffic to the affected areas; (see recommendation TF-MASIM-201304)

- Prioritisation of resumption of the communications of other critical infrastructures (power, transportation, financial, etc.) (such a recommendation could arise from TF-MASIM-201301, when the Expert group defines which Authority takes the lead and how it is determined);
- Critical nodes that may lack local generators need to be properly inventoried and this information shared; (see recommendation TF-MASIM-201301 and 02)
- Key nodes and ISP providers have local generators, but their fuel stock capacity may not allow the maintenance of generators running in the long term; (see recommendation TF-MASIM-201301 and 02)
- Specific risk analysis is not extensively carried out over environmental conditions of the local generators and oil tanks in those facilities having critical nodes of communications; (see recommendation TF-MASIM-201301)
- Very careful assessment of the switching operations between power -> batteries -> generators and vice-versa to avoid glitches that can harm the equipment and cause even worse impact. (see recommendation TF-MASIM-201301)

2.1.3 Mitigations

The Task Force identified some possible solutions to these issues. The list of these mitigations is not exhaustive, but provides already a number of key points to consider. Most of the recommendations could arise from the procedures decided by the Expert Group recommended in TF-MASIM-201301.

Alternative communications for FERs must not depend on affected infrastructure. i.e. Tetra/Tetrapol doesn't rely on the same infrastructures as commercial services;

- Policies for cross-border traffic prioritization should be developed and tested; (see recommendation TF-MASIM-201304)
- Emergency satellite communications terminals shared among several countries can be moved quickly to the affected areas by FERs to support the resuming of basic services;
- Voice and data service need to be provided to the Public. They could be supported by mobile modules (containers) that can be linked by means of satellite or radio;
- Ad-hoc networks which do not depend on fixed infrastructure should be deployed;
- Sharing of Materials (e.g. Mobile generators shared among several countries) can be moved quickly to those affected nodes or switching offices that doesn't have local generators;
- Management of Critical spare parts (for the power grid, some should be available for a period of time that will be in accordance with the requirements of the logistics of the critical nodes generators);
- Improve Public access to backup solutions (e.g. public charging batteries points for mobile phones and computers scattered in the cities).

While most of these measures may exist at National level, there might be significant differences from one Member State to another. The cross border dimension is rarely taken into account but could help save lives: for example, the transport of emergency telecom equipment to an affected region may be faster if this equipment is geographically closer but in a neighbour country.

Cooperation costs could be settled at a later stage.

2.2 Case Study 2: Loss of communication for dependent Critical Sectors, e.g. Finance sector

2.2.1 Description

A major power outage happens in Germany impacting areas in France, Luxembourg, Belgium and Netherlands:

- *Telecom Operators located in these countries have lost connectivity*
- *Several major Internet nodes are impacted;*
- *The Finance sector is impacted with delays in the processing of hundreds of thousands financial transactions;*
- *No victims directly due to power loss.*

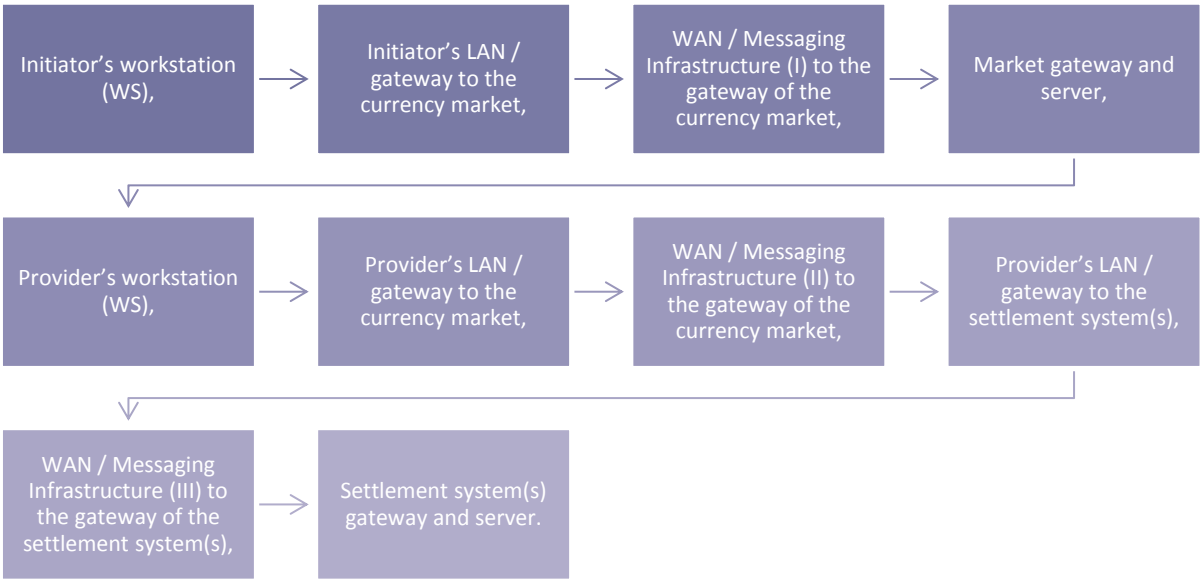
2.2.2 Impact Analysis

Cross border coordination in catastrophic situations at the pan-European level is missing and may heavily impact Critical Finance Infrastructures through communication failures. Currently, the crisis may see regulators acting more locally without collaborating in studying cross-border implications of catastrophes. New players in financial markets bring also new risks.

These new players (e.g. cloud service providers) result in a significant value shift from traditional banks to technological providers, so called “processors”, and a value share between banks and intermediaries. Technological openness additionally entails more intense competition with the risk that adequate security measures are neglected in order to benefit from easy and cheap alternatives. A more diversified banking and financial ecosystem with more players becomes a more fragmented systems with additional failures and incidents.

The needs may largely differ between banks and their customers, for instance, Banks are looking for a seamless provision of liquidities, while Bank customers are looking for 100% available and seamless end-to-end trade procedures as well as finality of transactions.

The transaction chain is executed via a number of "nodes":



Each one of these nodes relies entirely on electricity to operate. LAN, WAN gateways rely on electronic communications infrastructures, whether public or dedicated (privately leased).

Also, large customers were, at last, given access to interbank exchange systems like SWIFT, while medium- or small-size companies rely now also on Internet-based e-banking services, via their bank or via payment processors.

2.2.3 Possible Mitigations

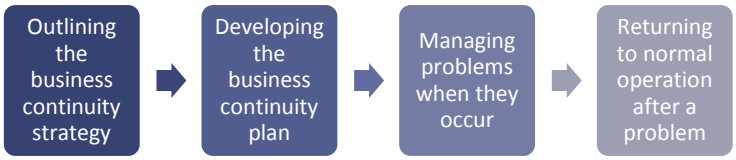
In response to the on-going trends, several infrastructures were put in place or modernised already. Also, Banks and their supply chain have established service contracts or service level agreements (SLAs).

For Banks, Incident Preparedness in their ICT Supply Chain is mostly achieved through their "Business Continuity Plans".

For the European Central Bank (ECB) draft glossary, "Business Continuity" consists of "arrangements aimed at ensuring that a system meets agreed service levels, even if one or more components of the system fail or if it is affected by an abnormal event."

In the financial sector, one of the leading authorities has been the Joint Forum, a group of IT Experts from Central banks worldwide, who are focussing on prevention and protection issues in the banking sector.

Dealing with business continuity will lead to activities that can progress along the following steps:



Regarding Business Continuity, MiFID obliges banks and other investment institutions to establish, implement and maintain a business continuity policy to ensure continuity of investment services in the case of an interruption of its systems and procedures. The major milestone reached by MiFID is the increasing importance of "a good practice" to a regulatory requirement that compliance responsibilities fall on the Board.

In parallel with that regulatory framework, several business continuity related security criteria, good practices and international standards have been issued (See the "Standards" section in the "References" chapter).

Mostly, for the Finance Sector, the reliance on ICT means also that unless the ICT providers are generally of poor reliability, their approach is currently to establish SLAs and no further compensate for a loss of connectivity.

In most cases, the "Management of the Incident" implies here that a critical Sector depending on ICT (and therefore on Energy) can only improve its preparedness to incidents, and consider appropriate Business Continuity measures to keep Operations running in Autonomy where possible.

2.3 Case Study 3: Technologic Implementation causing failure with Domino effect to competitors

2.3.1 Description

A major technological implementation fails and leads to a cascaded failure and later on, a large-scale outage, which impacts several millions of Users. Mobile Communications are mostly impacted; emergency services cannot be reached from GSM Networks.

There is no fallback scenario: no National Roaming is in place, Telecom operators have sometimes to intervene on sites to re-establish operations.

2.3.2 Impact Analysis

As mobile telecommunication networks are extremely complex systems comprising of thousands of service nodes of several different types, interfaced by diverse control protocols via hundreds of data elements, it is difficult to predict all the cascading effects of a single node failure. This cascading effect is made possible due to the relationships (also called dependencies) between the various components within the mobile telecommunication network. Cascading attacks are so named because local effects of corrupt data items propagates or cascades to data items on remote service

nodes through vehicles such as signalling messages, cached data items, and shared databases. When the cascade attack is originated outside of the 3G networks, i.e. the Internet as a launching pad, we refer it as a "cross infrastructure cyber-attack".

The impact of such attacks, among others, can lead to a Denial of Service or Interruption of the Service. In the case of Denial of the Service, the issue causes an overload or a disruption in the system such that network functions in an abnormal manner. The abnormal behaviour could be legitimate subscribers not receiving some of the services, illegitimate subscribers receiving services or even the entire network may be disabled as a result of the attack. In the Interruption scenario the issue causes an interruption by destroying resources, for example, the adversary may delete signalling messages, mislead or delete subscriber data in the entity such as a Home Location Register (HLR)[6].

2.3.3 Possible Mitigations

A vulnerability assessment toolkit should be used to be able to predict, not only all the diverse cascading effects of corruption but also detect the vulnerabilities that may be exploited to launch the attack.

Apply attack-graph technologies specifically designed to handle 3G semantics i.e. dependencies, and infection propagation rules. An attack graph is a diagrammatic representation of an attack on a real system. It shows the various ways an adversary may use to break-in to a system or cause corruption, and the various ways in which the corruption may propagate to remote parts of the network. Attack graphs are typically produced manually by “red teams”, and used by system administrators for protection. Model checking is a major technique for automatic attack graph generation. Logic-programming methods can be used for scalable network vulnerability analysis in terms of properties such as survivability, reliability, etc.

Standard network equipment configurations must be maintained centrally and audited daily. When needed, configuration updates go through a rigorous control change process, and then are downloaded from the Network Operations Center (NOC) at the company’s headquarters. These controls reduce the need for manual configuration of routers, switches, and other network elements, and lower the associated risk of error.

Mutual Aid Assistance is also considered as mitigation for this case.

A possible response lies in a few pragmatic steps:

- The use of multivendor technologies as well as the design of a compartmented network, either by regions or services, can help in quickly diagnosing, and avoiding the spread of the problem.

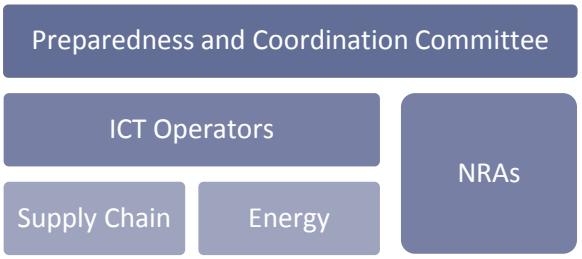
[6] http://commons.wikimedia.org/wiki/File:GSM_reseau.png

http://en.wikipedia.org/wiki/Home_Location_Register#Home_location_register_.28HLR.29

- The application of specific Contingency Planning Procedures as part of Business Continuity Plan. Exercises checking the ability of rollback procedures in order to restore to the previous stable state. (see recommendation TF-MASIM-201301 and 02)
- Regular Penetration testing checks from external networks towards both management system and signalling network, in 3G and LTE. (see recommendation TF-MASIM-201301)
- The usage of a syndication system of web feeds to broadcast, in real time, warnings and alerts about bugs, patches and change management, service support conditions or changes of the contact details of the key support staff. Privacy and security of such a system can be guaranteed through of tunnelling for communications channels and information rights management on the XML items. (see recommendation TF-MASIM-201302)

3 Recommendations

The situation in Europe (Borders, Market Concentration) creates a number of challenges that could be compensated by a set of control mechanisms. These mechanisms proposed are reported in the "recommendations" section, could allow addressing a number of the issues noted in the Case Studies.



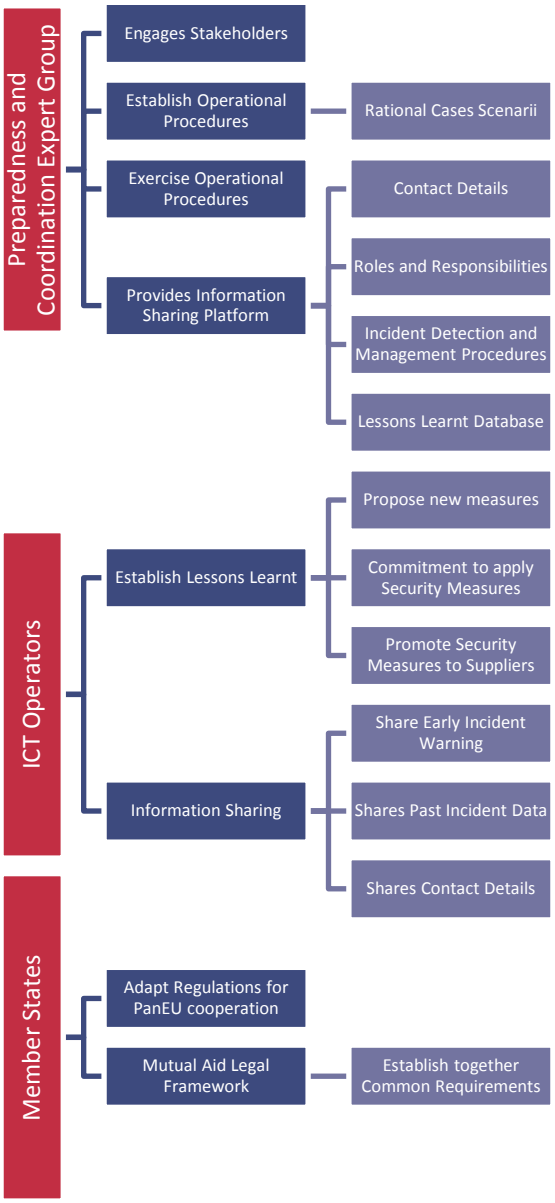
The Task Force felt that a dedicated horizontal organisation was missing, and considering the extent of the topics covered, its mission could last on the long term. Such a group does not need to be an initiative driven by the Public Sector: it could instead be volunteered and committed by Telecom Operators, organised in a Peer-to-Peer mode and self-committed to adopt relevant procedures and standards. The engagement of Public Sector would allow the implementation or adaptation of regulations where necessary. Furthermore, the Public Sectors' role would be to encourage the participation in such a pan-European group, and ensure that such information sharing cannot be seen as "anti-monopoly" type of agreement (which is usually forbidden and prosecuted).

All case studies and analyses converge to concluding that there is a strong urge to promote and facilitate pan-European cooperation on ICT Security matters in all CIIP-dependent sectors.

Those conclusions of the case studies intervene at several different levels, but have a number of common characteristics:

- They require a top-down implementation;
- They depend heavily on an Information Sharing platform;
- There must be a commitment to implement measures in a coordinated way;
- There must be a way to ensure the proper implementation of the measures.

The Observations above led to conclude on a number of initial steps to take so the topic could be later on widely addressed. The recommendations typically address each of the three domains identified in the initial scope (Information Sharing, Mutual Aid, Technology Convergence & Interoperability) and fit globally within the Expert Group that is the first recommendation of the Task Force, as a horizontal condition.



This report therefore raises first a number of important recommendations to consider as a priority:

- Systematic and Compulsory Information Sharing for Incident Preparedness needs to be established, such as:
  - Incident Response Procedures vis-à-vis the external world;
  - Key Emergency Contacts of ICT-sector public and private actors details shared among all key actors and maintained up to date at European level;
  - Roles and Responsibilities of all actors (after being defined);
- Incident Information needs to be collected and analysed to rationalise prevention costs;
- For medium sized incidents, a lighter process such as Mutual-Aid mechanism could be promoted in a cross-border de-regulated bubble (with finite timeframe of operation).

These recommendations are further developed below.

3.1 EP3R-TF-MASIM 201301 – Establish a 'Incident Preparedness and Coordination Expert Group'

The Task Force recommends to the Telecom Operators, ICT Stakeholders, the European Commission and the Member States to initiate the creation of a Pan-European Expert Group with Operational capabilities, where key stakeholders can formally plan and organise both Strategic and Operational functions of Incident Preparedness procedures.

A top-down approach is recommended: Senior Executives and Public Decision makers should initiate the commitment and define clear objectives.

The key objective is the pursuit of faster recovery and the avoidance of the Tail-Event Syndrome7 i.e. which is only reacting after the incident happens, lacking preparedness, and not being able to manage events timely.

The core mission of this Expert Group should be to address all Incident Preparedness Prerequisites that need to be dealt with horizontally, with a cross-border dimension.

Initially, the following actions were considered and recommended by the Task Force:

- Engage and commit Key European ICT Stakeholders in discussions;
- Establish Operational Pan-European Incident Response Procedures;
- Implement an Information Sharing Platform for Incidents Early Warning;
- Establish and share centrally Procedures, and Key Responsible Contact Details;
- Plan the Exercising of these functions.

At a later stage, the Expert Group could deal with more complex issues, after issuing a detailed roadmap. Some tasks are crucial in this approach, such as ensuring Actors' self-commitment to implement them, coordinating and harmonising National Contingency Plans, defining guidelines for establishing Business Continuity Plans, harmonising Incident Detection measures, promoting the establishment of Mutual Assistance agreements, etc.

Such an Expert Group membership should be composed of representatives of:

- European telecom operators;
- European NRAs;
- CERTs;
- European Commission.

[7] MARIE Phase I report: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

3.2 EP3R-TF-MASIM 201302 – Implement a RSS-syndication type of platform for sharing Incidents Preparedness procedures, Early Warnings, and Contact details

The Task Force highlighted the need for a private initiative for Telecom Operators and CII Stakeholders to implement a systematic sharing of information. Currently, Telecom Operators generally consider the sharing of information as potentially damageable to competition, and in some cases (e.g. for the set of prices), such an exchange could be considered illegal and a jeopardy of competition rules.

The sharing of technical incidents data should however not be considered as hindering anti-monopoly rules, on the contrary: such a sharing of information would benefit immediately the Citizens since Incident Preparedness allows a much faster recovery.

The data that should be shared potentially relates to:

- Incident Preparedness Procedures;
- Cooperation Details (Mutual Aid Assistance Agreements);
- Emergency Response Procedures;
- Emergency Contact Details;
- Incident Early Warning.

This platform could implement the Functional, Management requirements and recommendations of the EP3R Task Force on Trusted Information Sharing, and allow a closed community of Telecom Operators' representatives, Security Officers, Network Managers, IT Production Managers, Business Continuity Coordinators and Managers to share IT Security and Risk Management relevant information.

A syndication mechanism could also technically implement a distribution of information updates to all members via a pseudo-push mechanism, and therefore spread changes easily to avoid obsolete records stored at local sites. Such a centralised system could be of great value to Telecom Operators, and was actually proposed by one major European Telecom Operator during the Task Forces discussions.

3.3 EP3R-TF-MASIM 201303 - Establish a Favourable pan-European environment for Mutual Aid Assistance

Mutual-Aid Assistance was perceived within the Task Force as a "Quick-Win".

Such framework is easy to establish, could allow an initiation of regular contacts between ICT Stakeholders and later develop cooperation on larger assignments.

The key recommendations from the Task Force are to:

- Promote the use of Mutual Aid Assistance (MAA) across Europe;

- Develop a MAA template / catalogue where possible topics are listed (and therefore not forgotten);
- Ensure MAAs are endorsed, supported and promoted by Public Authorities and Regulators.

The MARIE Phase II report also lists a number of more specific requirements and recommended approach[8] that the Task Force endorses fully.

3.4 EP3R-TF-MASIM 201304 - Policies for cross-border traffic prioritisation should be developed and tested

On the technological side, the Task Force noted that one of the most important technological issues in Europe concerns the dismissal of Priority Calling Scheme when calls are routed cross border (and in some cases between operators). The ENISA Report on National Roaming[9] also recommends traffic prioritisation at national level (and also favours Mutual Aid Agreements). This recommendation adds the cross border dimension.

Compared to Foreign Continents/Countries[10], a disaster involving several countries may be extremely complex to resolve, and since such a scheme is not in place, the odds that important communications reach the First Emergency Responders is decreased and possibly fully compromised.

8https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

9http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/national-roaming-for-resilience

10 http://transition.fcc.gov/pshs/techtopics/techtopics18.html

4 Conclusion

Improving Incident preparedness at pan-European level implies that a global cross-border dialogue emerges in Europe and that every key actor actually engages and commits to an implementation roadmap.

The overall process could be driven top-down by the European Commission, but it is more likely that a Peer-to-Peer approach based on Self Commitment works better: indeed, the incentives are mainly financial, since they tend to reduce recovery time for ICT Operators.

The Expert Group should develop a portfolio of Strategic, Governance, and Technical tools which will improve cross-border incident preparedness. Such platform for effective Information Sharing, Mutual Aid Assistance, and allow proper Technological Interoperability.

Formalising such a partnership will however require solutions to a number of challenges and barriers, for instance:

- Regulatory fragmentation preventing effecting cross-border information sharing on Security and Resilience topics;
- Non-Disclosure Agreements, to ensure Security and Preparedness matters are never considered a competitive advantage;
- Ensure Information Sharing cross border is not considered illegal or Competitive pre-agreement (which is against anti-monopoly rules);

In some cases, the solutions recommended will also require operational capabilities, which should be the responsibility of a neutral body or institution. The solutions should then be then envisaged in a pragmatic way. Possibly, the European Commission may be the most appropriate Authority to solve certain issues together with Member States, but the needs will lead to raising recommendations where appropriate.

References

Standards

BCI — The BCI Good Practice Guidelines

BSI — Business continuity management Specification (BS25999-1:2006, BS 25999-2:2007)

BSI — BS 25777:2008, Information and communications technology continuity management. Code of practice

International Organization for Standardization

ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management

ISO/IEC 22399:2007, Societal security - Guideline for incident preparedness and operational continuity management

ISO/IEC 24762:2008, Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services

National Institute of Standards and Technology (NIST) SP 800-34

NFPA 1600 — Standard on Disaster/Emergency Management and Business Continuity Programs (2007 Edition)

Related ENISA papers

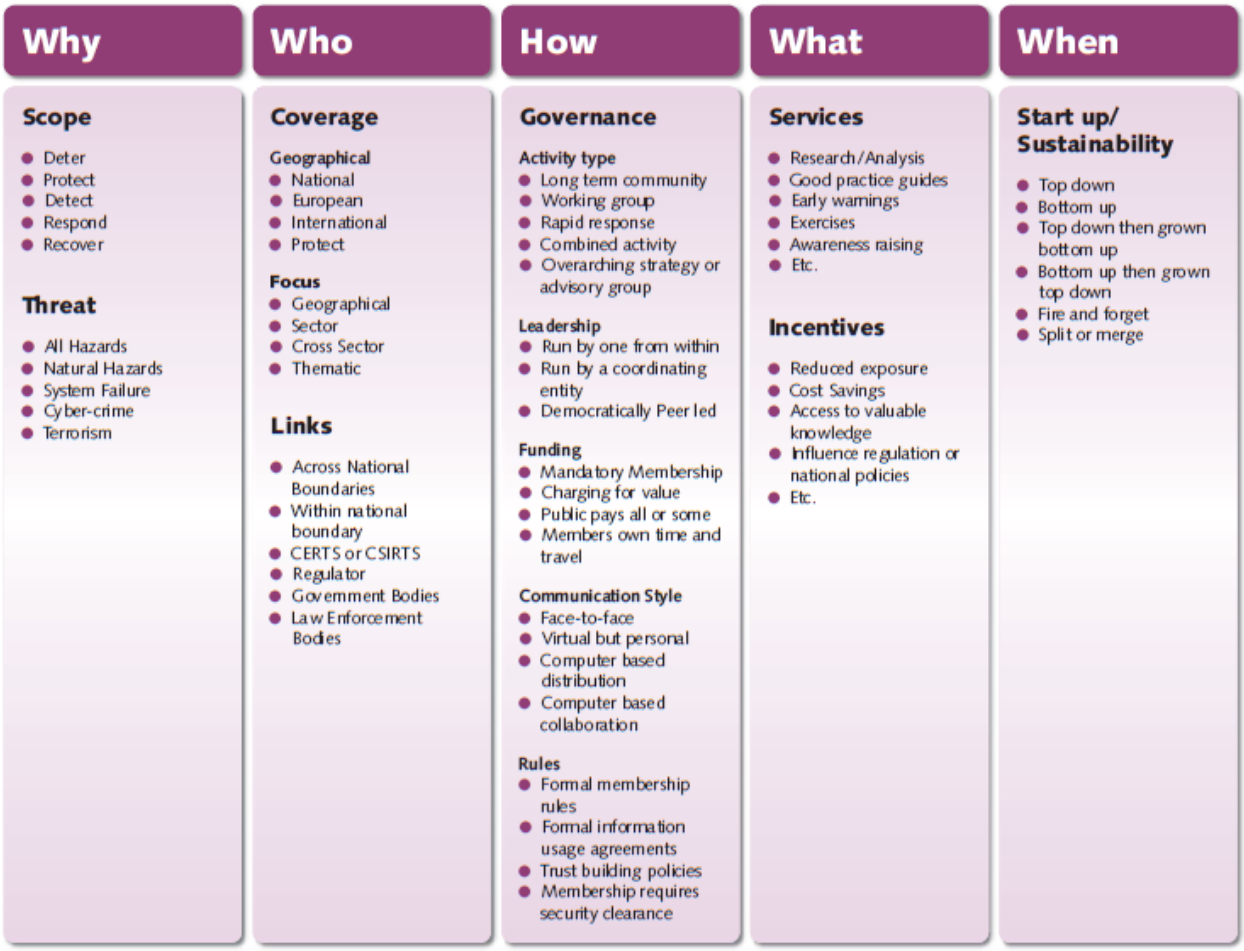
Mutual Aid for Resilient Infrastructure in Europe: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

Other Publications

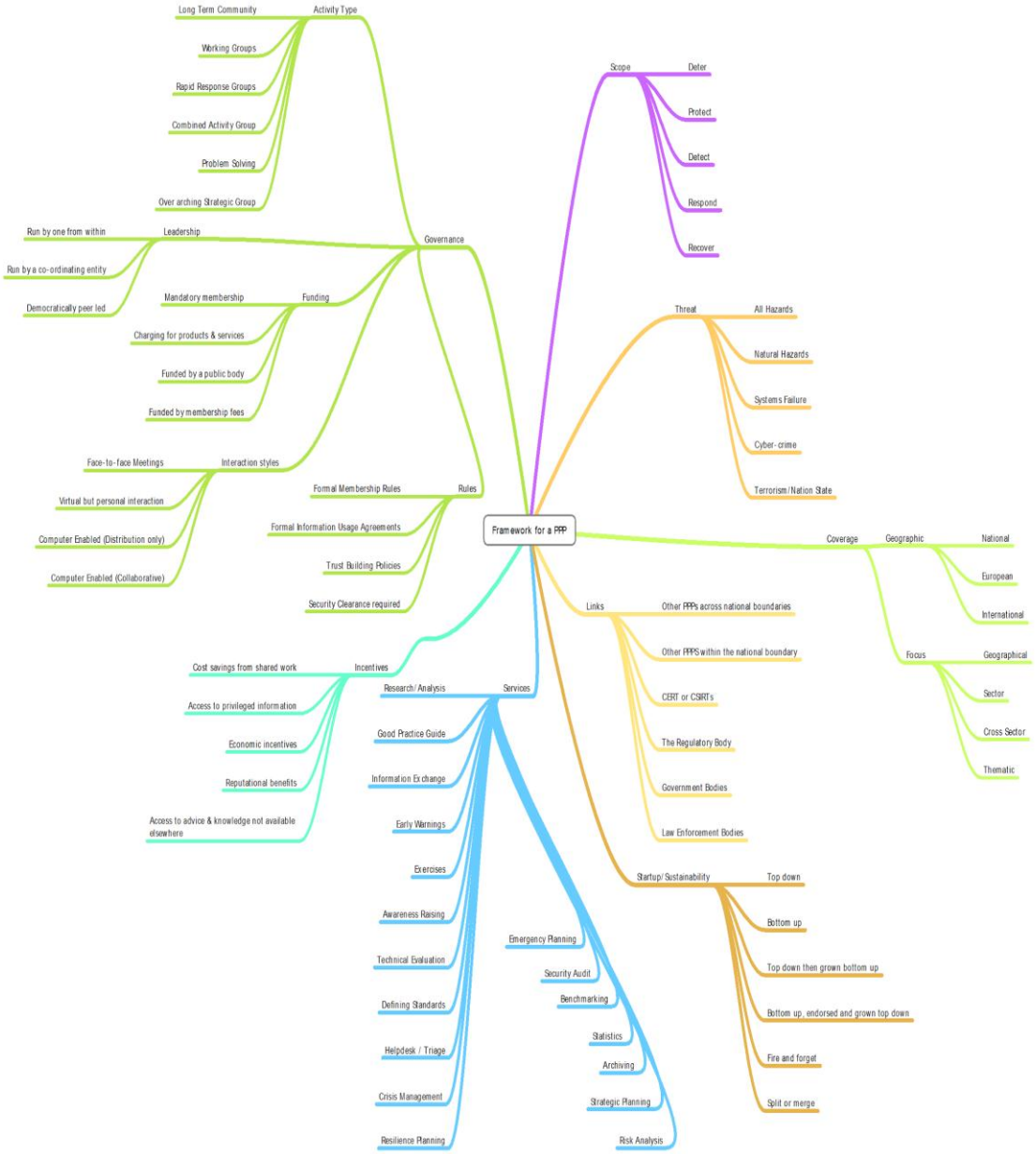
Karl F. Rauscher, Richard E. Krock, and James P. Runyon, 2006, Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal, (c) Lucent Technologies Inc. Downloaded from: www3.alcatel-lucent.com/enrich/v1i22007/pdf/BLTJ_20179.pdf

Annex A: PPP 5 Pillars

This figure shows the key characteristics of a Partnership.



Annex B: PPP Framework



Source: Good Practice Guide on Cooperative Models for Effective Public Private Partnerships (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps)

Annex C: 8 Ingredients for Mutual Aid

Karl F. Rauscher, Richard E. Krock, and James P. Runyon, 2006, Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security, Bell Labs Technical Journal, (c) Lucent Technologies Inc.

Downloaded from: www3.alcatel-lucent.com/enrich/v1i22007/pdf/BLTJ_20179.pdf

Ingredient	Example of Asset
Environment	space in a strategically located data centre
Power	diesel generator
Hardware	cell on wheels (COW)
Software	program on hardware provided (above)
Network	spare critical ingress or egress capacity
Payload	creating, processing, storing or transporting data
Human	cable splicer
ASPR	Agreements, Standards, Policy and Regulation

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu