RISK AND RESILIENCE REPORT 9

Measuring Critical Infrastructure Resilience: Possible Indicators

Zurich, April 2015

Risk and Resilience Research Group
Center for Security Studies (CSS), ETH Zürich

Commissioned by the Federal Office for Civil Protection (FOCP)

CSS
ETH Zurich

ETH zürich

Author: Tim Prior

Center for Security Studies (CSS)
ETH Zurich
Haldeneggsteig 4, IFW
CH – 8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
Fax: +41-44-632 19 41
css@sipo.gess.ethz.ch
www.css.ethz.ch

Contracting Entity: Federal Office for Civil Protection (FOCP)
Project lead FOCP: Stefan Brem, Head Risk Analysis and Research Coordination
Contractor: Center for Security Studies (CSS), ETH Zürich
Project supervision CSS: Tim Prior, Head Risk and Resilience Research Group; Oliver Thränert Head, Think Tank; Andreas Wenger, Director CSS

Suggested citation: Prior, T. (2014): Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Report 9, Center for Security Studies, ETH Zürich.

Table of contents

1 Introduction

The concept and approach of resilience is gaining traction in Swiss civil protection and critical infrastructure protection policy. The main goal of the Swiss National Strategy for Critical Infrastructure Protection (CIP) highlights that Switzerland should become "resilient in relation to critical infrastructure to prevent large scale and catastrophic failure, and to ensure the extent of damage is minimised." A key step in realising this goal in the near future will be the development of one (or several) means by which to assess resilience so that progress towards the goal can be discerned.

This Risk and Resilience Report follows directly from the previous report on "Measuring Resilience: Benefits and Limitations of Resilience Indices" (Number 8)[1]. It provided a background to the issue of assessment – openning a discussion about the assessment of resilience and exploring the reasons why resilience might or should be assessed. This present report aims to illustrate how resilience might be assessed, and to elucidate indicators that might be useable in the context of Swiss CIP.

The report procedes to explain the differences between absolute and relative assessments of resilience in section 2. In section 3 it outlines a selection of indicators that might be used to assess critical infrastructure (CI) resilience and articulate the application of these indicators. Section 4 details two case studies where resilience indices have been developed based on a number of specific indicators. In this section, the methodologies are explored, particularly highlighting some possible advantages and disadvantages of both CI resilience exercises. Finally, section 5 places all this information in the context of CI resilience in Switzerland, particularly reflecting on important issues that must be considered in assessment and ongoing research.

2 Absolute or relative assessment of resilience

Resilience is fundamentally a theoretical concept. Yet ongoing and warranted reflection regarding this concept in the context of disaster and emergency management and mitigation, crisis management, and the protection of critical infrastructures, for instance, has thrust this concept into the policy making arena, where considerations concerning its practical application are becoming important. While difficult, given the complexity of resilience[1–4], and its definitional ambiguity[5–7], the ability to assess such a concept helps to bridge the gap between theory and application[8], between academic and policy circles.

Previous Risk and Resilience reports have discussed both the complexity of resilience and the challenges associated with defining the concept[9–11]. These reports also illustrate that measuring resilience is complicated, particularly in relation to bridging the gap between theory and application. Much of this complication is influenced by the unavoidable fact that the assessed resilience of any critical infrastructure is likely to be determined by a (huge) range of factors: physical, social, organisational, institutional, and cultural. Illustrating the significance, difficulty and resource intensity of measuring complex multi-functional phenomena like the resilience of critical infrastructure, Petit *et al.*[12] describe a resilience index built around the composition of 1700 unique points of data.[2] Realistically, such an involved process is next to impossible without significant and dedicated financial resourcing.[3]

Just as important in bridging the theory-policy making gap in relation to measuring resilience is the fact that many components of resilience are hard to characterise and hard to assess. In this context it is important to distinguish between developing a resilience 'measure' and developing a resilience 'index'. On the one hand, a measure can be defined as an 'definite or known quantity', while an index is a 'pointer or indicator'. Important differences exist between these two terms that have implications for the way the resilience of a CI is assessed. As a definite or known quantity, a measure is an absolute reflection of the subject being examined. However, an index is merely an indicator, yielding only a proximal representation of the actual subject under assessment. For this reason indices only yield a relative assessment (how is the entity changing relative to other entities assessed using the same indicator?), rather than an absolute measure.

A relative assessment is not exact, and depending on the rigour of the development process, may not explain a lot about the actual resilience of the entity of interest. However, as long as the index is calculated consistently between entities (of the same or very similar nature), all the index allows is a comparison between those entities, or over time. This is appropriate if only a relational understanding of resilience is required (for example, to allocate resilience development funding, or to highlight differences between the indexed resilience of structures). Using an index, or relative assessment of resilience is undoubtedly useful, but influences the

1 Prior T, Hagmann J. Measuring Resilience: Benefits and Limitations of Resilience Indices. Center for Security Studies: ETH Zürich, 2012 Contract No.: Focal Report 8: SKI.

2 The selection of indicators and development of this resilience assessment methodology is explored in greater detail in section 4.1.

3 The Enhanced Critical Infrastructure Protection Program cost the US Department of Homeland Security USD 27.5 million in 2012.

methodology of assessment, and has implications in the ultimate use of the results.

One way to avoid the problems associated with relative assessments of complex characteristics like resilience is to benchmark assessments against known measures.[14] Benchmarking determines the baseline conditions of normal function for an entity. Clearly, these conditions will be specific for different entities, but once baseline or 'normal' conditions are known, then assessed changes in an index can be compared to the baseline state of the entity.

However, if an accurate or absolute measure of resilience is required, then an index will be insufficient for the task. As Lonergan *et al*.[13] point out, an index assessment may not provide insight into changes in the indicated entity (like resilience), but only relative changes arising as a result of the changing status of other entities. An absolute measure of resilience (or any other characteristic) in an entity gives an exact measure of that entity's resilience. The determination of whether an absolute measure or relative assessment of resilience is used must be an early consideration, and made at the same time as considerations about why and how resilience is assessed, and what the results of the assessment will be used for.

Indices are more widely utilised than absolute measures, principally because an absolute measure requires a fundamentally deeper understanding, and 'bullet-proof' definition of the characteristic being examined. Resilience is a complex concept, which is undergoing continual refinement and even redefinition. For this reason, knowing *what* to examine when assessing resilience is often an unanswered question. An index is a way of simplifying the complexity. Indices are typically derived from several (or many) indicators whose relationship to the focus of the index are assumed to be representative. Indicators represent components of the subject of assessment – in the case of infrastructure resilience, these include features like functionality return time, redundancy, resistance, *etc*. – which are discussed in the following section. Thus, by assessing the indicators, often weighting[4] more heavily those indicators known to be more closely related to the subject of assessment, an index can be created.

4 Weighting: in statistical terms a 'weighting' is defined as a coefficient assigned in a computation to make the number's effect on the computation reflect its importance. An indicator that more closely reflects an aspect of resilience may be assigned a heavier weighting to express its importance in the calculation of the resilience index.

3 Potential critical infrastructure resilience assessment indicators

The indicators used when assessing resilience depend heavily on the resilience context under question. As highlighted in previous Risk and Resilience reports and fact sheets, resilience has been used quite differently across a broad variety of social, technical and economic disciplines. For example, the indicators used to assess psychological resilience differ so greatly from those used to assess CI resilience (because psychological and critical infrastructure resilience are vastly different) that, while both are termed resilience, a focus on the indicators used to assess them may show that they are two fundamentally different characteristics.

In this section, the report concentrates on identifying and describing indicators that could be used to assess CI resilience. It also examines the development of two CI resilience indices (section 4). Typically, CI resilience indicators can be classified in relation to a shock or disturbance. Some are applied in an *a-priori* manner, giving a relative assessment of resilience before, and independent from, a shock or disturbance. Others are used in a *post-hoc* manner, often giving an absolute measure of the indicator that is directly benchmarked against a predetermined baseline, and assessed following some shock or disturbance.

In addition to the specific *a-priori/post-hoc* separation articulated below, assessing resilience can also be generically classified. Four characteristics in particular have been used to describe the nature of resilience in cristical infrastructure particularly:[15]

- Robustness: a system or system component's resistance to loss of function in the event of a disturbance or shock.
- Redundancy: the level of substitutability of a system or system component, where functional service can be maintained
- Resourcefulness: the ability to direct resources to support a system or system component to increase robustness in the event of a disturbance or shock.
- Rapidity: the restoration of functionality in a timely manner.

Although these terms are widely used in discussions about the assessment of CI resilience, their generic nature yields limited practical application power in realistic assessments of CI resilience. In addititon, like resilience itself, different authors define these characteristis differently, or omit one from their examinations such that the consistent use of the same terminology is rarely obvious. For these reasons, a more specific identification and

description of CI indicators is provided in this section. Indeed, many are subordinate to the four more generic classifications listed above.

The list of specific indicators described in this section is by no means exhaustive, but is provided to illustrate the type and variety of indicators that may be engaged in the assessment of CI resilience. This report does not detail the methodologies to collect data for each of the indicators – this should be undertaken in consultation with technical specialists and infrastructure managers. Typically, the type of infrastructure will determine the type of data collected and collection methodology for each of the indicators listed here, meaning also that resilience may need to be measured on an object basis, relying on relational indices for comparison.

3.1 *A-priori* critical infrastructure resilience indicators

3.1.1 Probability of failure

Probability of failure is an estimation of the expected impact and degradation of an infrastructure following a disturbance or shock.[16] This probability will vary depending on the nature of the disturbance or shock, but also on the nature of the infrastructure itself. For example, design faults, inadequate maintenance, long service and aging materials[17] will all influence the speed and susceptibility of failure, and the magnitude of failure. Probability of failure can also be influenced by organisational or management deficiencies that may influence the quality of pre-disturbance planning.

3.1.2 Quality of infrastructure

Quality of infrastructure is an indicator of how well an infrastruture performs. Performance is influenced by design, materials used, age, service life, and the quality of management and maintenance. Infrastructures with lower quality are likely to be less operable following disturbance, and this indicator can be used to describe performance over time. Quality of infrastructure may be assessed using a 'satisfaction of service' proxy, where greater satisfaction reflects higher quality.

3.1.3 Pre-event functionality of the infrastructure

Assessing pre-event functionality is an important benchmarking exercise that can be used to inform resilience based on how rapidly CI function returns following disturbance. Knowing the baseline level of functionality of a CI is fundamental to assessing and quantifying functionality change both in normal operational circumstances, but especially following a disruption (see section 3.2.3). Functionality can also be considered a proxy for the quality of the infrastructure – higher quality infrastructure generally functions better, and therefore may be less likely to fail if subjected to disturbances or shocks that it has been designed to cope with.

3.1.4 Substitutability

Substitutability is an aspect of a CI system's redundancy, and a key characteristic associated with resilience in infrastructure. Substitutability reflects the possibility that the functional aspects of an infrastructure or infrastructure system can be replaced by back-up infrastructure or by other components in the system.[15, 16] Assessing inherent substitutability for an infrastructure, or in an infrastructure system, can yield important information that informs the allocation of resources for infrastructure protection (resources may be more effectively allocated for the protection of infrastructure where a substitute is not readily available or in existence), or improving infrastructure quality.

3.1.5 Interdependence

Modern infrastructure systems are complex and in many cases are characterised by extensive interdependencies. On the one hand, interdependencies may confer an advantage if those relationships increase the functionality and/or substitutability of the infrastructure. On the other hand, interdependence may be a disadvantage if reliance on the relationships is essential for one or many components in the system. Ulieru[4] also highlights the existence of 'critical hubs' in interdependent systems, and in the case of infrastructure the disruption of such hubs may incite unavoidable system collapse. Assessing where interdependence exists, the nature of the relationships, and the criticality of the connections are important pre-disturbance endeavours that can be useful indicators of CI resilience. Classifying interdependencies as either physical, cyber, geographic or logical (interdependence is not characterised as one of the previous three states)[18] can also help to assess this indicator of resilience (or vulnerability).

3.1.6 Quality/extent of mitigating features

Assessing the quality and extent of features associated with an infrastructure that can mitigate the consequences of disturbance or shock is an important *a-priori* resilience indicator. Mitigating features add to the robustness of the infrastructure, and an early assessment of their quality and extent can be useful in improving these features where the necessity exists. Mitigating features will be specific both to the type of infrastructure and the nature of disturbance the infrastructure is likely to be subject to. Mitigating features might include organisational, hardware or software systems that ensure functionality,[19] and that should also be capable of adapting to changing extrinsic (outside of the infrastructure) and intrinsic (internal to the infrastructure) conditions.

3.1.7 Quality of disturbance planning/response

Technical assessments of infrastructure are perhaps the most obvious when considering resilience, yet considering organisational planning for preparedness and response are also important. Assessing the value of pre-determined policies that increase or maintain the quality and functionality of infrastructure can be a useful indicator of resilience. In addition, the nature and availability of repair facilities, resources or personnel can also increase the speed of recovery (see section 3.2.6) following disturbance, therefore playing a significant role in CI resilience.[19]

3.1.8 Quality of crisis communications/information sharing

The quality and nature of crisis communication structures, and organisational information sharing between managers of CI and government agencies can be a useful indicator of the CI resilience. Where crisis communication methodologies and technologies are of high quality and functionality, their deployment at times of disturbance or shock may limit loss of functionality, and speed up the recovery of infrastructure function. Making either qualitative or quantitative assessments of information sharing processes and practices can be particularly good indicators of the strength of relationships of the managers of infrastructure systems that are characterised by significant interdependencies.

3.1.9 Security of infrastructure

Modern risks from terrorism or cyber attack on critical infrastructure means that security of, and around, CI is of increasing importance. Security in the form of physical structures (fences, lighting, *etc.*), security management (security planning, communications, *etc.*), or personnel (security force, training, *etc.*) may decrease the likelihood that infrastructure fails or loses functionality.[20] Making assessments of the security of an infrastructure can be an informative means of understanding whether the infrastructure could be vulnerable, and addressing vulnerability can lead to increased resilience (but not always, as the relationship between resilience and vulnerability is not always a direct one, an issue that has been discussed elsewhere[9, 10, 21, 22]).

3.2 *Post-hoc* critical infrastructure resilience indicators

3.2.1 Systems failure

Observing an actual failure in an infrastructure can provide a clear indication of its resilience, and specifically what characteristic of the infrastructure, or its relationship to the disturbance, may have led to the failure. Many factors may influence the likelihood that a system fails completely, including those factors outlined in 3.1.1, but also interdependencies, lack of security, poor management and disturbance planning, poor communications, *etc.* Systems failure can be measured in a binary fashion: fail, or not fail.

3.2.2 Severity of failure

Factors described in 3.1.1 above will also influence how severely an infrastructure fails. For instance, old or poorly maintained infrastructures are likely to fail such that they lose functionality completely following disturbance, and consequently require a complete rebuild during recovery.[19] By contrast, well managed, newer infrastructure that is designed to cope with disturbance (the most likely to occur in any given location) is likely to suffer less as a result of disturbance, and some functionality may persist.

3.2.3 Post-event functionality

Measuring functionality of an infrastructure following a disturbance or shock, and comparing this level to the pre-event assessment of functionality will provide an excellent indication of CI resilience. The closer the level of post-event functionality to the assessed pre-event functionality, the more likely the infrastructure is to be resilient (in relation to a consequential disturbance). In addition, the speed at which pre-event functionality can be restored following a disturbance, based on aspects like the quality of planning, communications, mitigation features, and the quality of the infrastructure, can also indicate strong CI resilience (see 3.2.6).

3.2.4 Post-event damage assessment

Geographic information systems (GIS) and remote sensing technologies can, and have been used in post disaster damage assessments.[15] Such technologies can be used to yield quantitative measures of damage to many forms of infrastructure, and therefore give a direct idea of the robustness of infrastructure affected by the disturbance. For example, the Multidisciplinary Center for Earthquake Engineering Research in Buffalo, New York, uses satellite images to determine the location, and severity of building damage following an earthquake.[15] The information is extremely accurate, and when compared to information about the age, quality, maintenance and management status of an infrastructure, can provide an idea of the infrastructure's resilience to earthquake.

3.2.5 Cost of reinstating functionality post-event

The cost of returning infrastructure to pre-event functionality can be used as an indirect measure of an infrastructure's resilience. This measure assumes that a greater expense (relative to the value of the infrastructure alone, not the value of the service the infrastructure provides to society) equates to more damage, and therefore lower resilience in the infrastructure.

3.2.6 Recovery time post-event

Possibly the most well-known indicator of resilience in CI, the recovery time post-event is a measure of the amount of time it takes for an infrastructure to be brought back to its pre-event level of functionality.

3.2.7 Recovery/loss ratio

Closely related to 'recovery time post-event'[3.2.6], the recovery/loss ratio is a calculation of speed of recovery based on the severity of loss. More severe loss, or decrease in functionality, would generally be associated with a longer recovery time. However, for CI that is rated as having a high level of resilience, the speed at which recovery occurs may be higher than similar infrastructure with lower rated resilience. This ratio is consistent with the 'bounce back' notion of resilience, in that where recovery and loss are equal an infrastructure is fully resilient, but where no recovery is exhibited, then resilience is also absent.[19]

4 Case comparison: Development of resilience indices

CI resilience cannot be assessed by examining indicators such as those described above in isolation. These indicators are strongly interconnected, and a quantification of CI resilience requires an indexed calculation, based on the weighted importance of each indicator. Drawing these indicators together into a meaningful index is not a simple task, and this section details two examples of the application of a CI resilience index in practice. The following examples used are not necessarily best practice, but are examined in order to illustrate different methodologies to identify indicators and aggregate them into an index.

4.1 Enhanced Critical Infrastructure Program[5]: Resilience Index

The Enhanced Critical Infrastructure Program (ECIP) is perhaps the US Department of Homeland Security's most visible CIP partnership. The objective of the ECIP is the collection of information on vulnerability and criticality of a variety of critical infrastructure and key resources (CIKR). It is object-focused. This information is used to benchmark the security of CIKR assets, to compare security between similar infrastructures or resources, and to provide the operators of these CIKR with timely and useful information that can improve the security management of the assets.

Initially the ECIP was used to collect information on vulnerability (Vulnerability Index) and security (Protective Measures Index).[20] However, these measures do not give an indication of the likely consequences CI or key resources may suffer if they are struck by a disturbance or shock. To address this shortfall, the Department of Homeland Security has invested in the development of a Resilience Index (RI), which aims to "generate reproducible results that can support decision-making related to risk management, disaster response, and maintaining business continuity" of critical infrastructures and key resources.[12] The fundamental goal of the RI is to understand the ability of CI to offset the magnitude and duration of a disturbance event. The Index is used as a benchmark against which to direct infrastructure investments that improve the resilience of the infrastructure.

4.1.1 Development and indicators

The RI is developed using a hierarchical process, placing the generic characteristics of resilience at the uppermost "Level 1': robustness, recovery and resourcefulness. Information is collected for components at four further levels organised below this, and reflecting ever-increasing specificity. At 'Level 2', information is collected for three components signifying robustness (redundancy, prevention/mitigation, and maintaining key functions), two components signifying recovery (restoration and coordination), and for seven components signifying resourcefulness (including training/exercises, awareness, protective measures, *etc.*). 'Raw' data is collected for 47 components at 'Level 3', and these components are defined by subject matter experts who have been specifically consulted in the RI development process.

4.1.2 Methodology

Data is collected using a survey instrument completed by trained personnel in partnership with a responsible manager of the infrastructure being assessed. Data for every component and subcomponent is weighted based on its relative importance, when compared to the other components or subcomponents at its level. The process of weighting is conducted by subject area specialists in cooperation with representatives from the infrastructure sector under question. Weighted scores are aggregated at each level, starting from the lowest level and finishing at the three-component 'Level 1'. The final added score is used as the RI value. Figure 1 illustrates the organization of the first two levels of the Resilience Index.

4.1.3 Advantages and/or disadvantages

The hierarchical nature of the assessment technique enables data to be collected for very specific aspects of

5 The full Enhanced Critical Infrastructure Program (ECIP) is described in SKI Focal Report 8: Measuring resilience: benefits and limitations of resilience indices. See also *http://www.dis.anl.gov/projects/ri.html*.

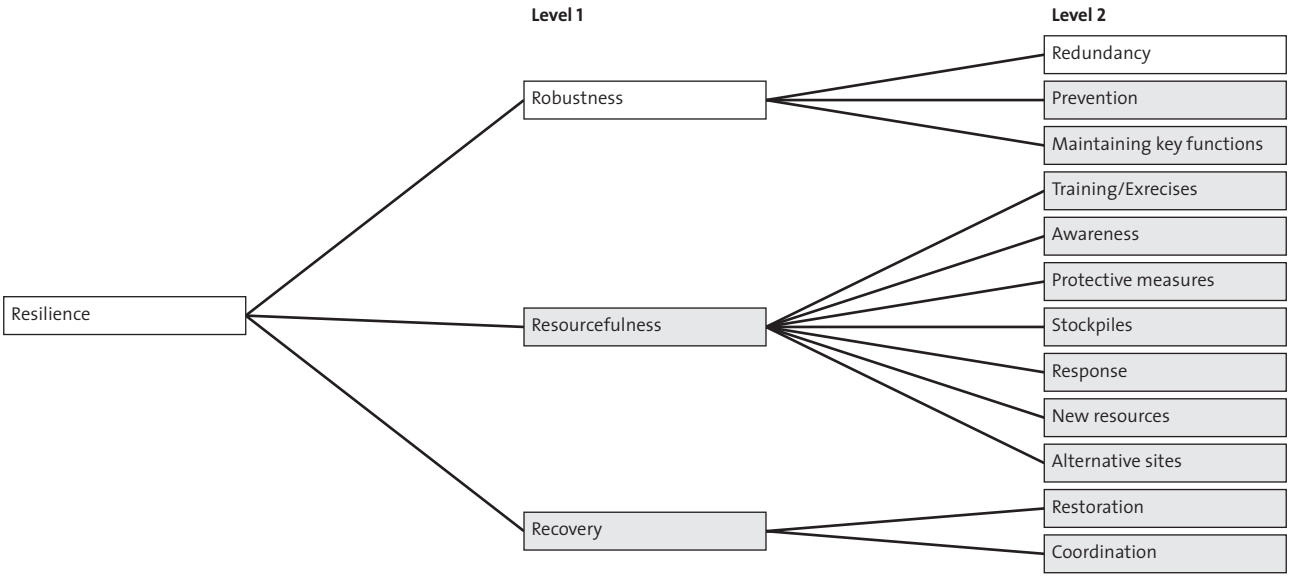

Figure 1: Resilience components at levels 1 and 2 of the ECIP Resilience Index (from Fisher *et al.*, 2010).

resilience, and aggregated into a composite index. The resulting index provides only a relative assessment of resilience in the infrastructure in question, and can therefore only be used comparatively against similar infrastructures, or to illustrate how resilience changes over time in one infrastructure.

However, the data collected at the sub-component level provides a very fine illustration of particular aspects of the infrastructure that contribute to its overall resilience. These sub-components are identified by subject area experts and infrastructure operators, and examining these closely can highlight where effort or investment might be most valuable in pushing up the aggregate resilience assessment. Fisher *et al.*[23] illustrate that specific answers to survey questions at the finest levels can impact on the resilience component levels further up the index's organizational hierarchy, demonstrating where important investments or changes in infrastructure may have consequential benefits for the infrastructure's overall resilience. For a detailed explanation of the calculation of the resilience index refer to Fisher *et al.*[23] and to Petit *et al.*[12]

4.2 Resilience of the trans-oceanic telecommunications system

Omer and colleagues[24] developed a network model to assess the resilience of the trans-oceanic telecommunications system (Figure 2). This infrastructure system permits global information sharing, and consequently supports international communication traffic that is the basis of the modern global economy. The infrastructure is composed of fibre optic cables laid on the seafloor. Although the cables themselves are reasonably robust, they are vulnerable to a number of disturbances: dropped anchors, trawling nets, natural hazards, deep sea wildlife, and seawater.[24]

The network model used in this assessment of resilience is useful because, like telecommunications, many forms of modern infrastructure are built up on networks: roads, energy and water supply grids, for example. As such, this methodology may also be feasible for other forms of networked infrastructure. While the general methodology may be replicated, different indicators of assessment would be required for the various infrastructure applications.

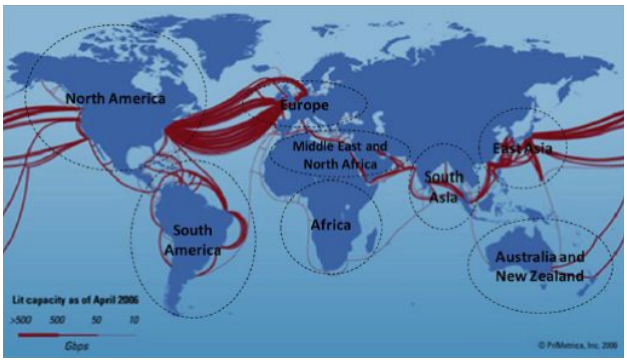

Figure 2: Global trans-ocean telecommunications infrastructure (From Omer *et al.*, 2009).

4.2.1 Development and indicators

The measurement of resilience in this instance is based on two variables. Firstly, resilience is determined partly by the network's value delivery. Resilience is considered high if value delivery following a disturbance is close to or equal to the value delivery pre-disturbance. 'Value delivery' is a representation of the total amount of information that must pass through the infrastructure. Resilience is secondarily characterized by the value delivery between 'nodes' in the system. 'Node to node resiliency', as

it is termed, is an individual calculation of the value delivery between two nodes before and after a disturbance. Aside from these variables, data on node demand (quantity of information travelling through a node, link capacity (total amount of information a fibre cable can carry), and lastly, the traffic flow (the proportion of a link's total capacity used at any one time).

4.2.2 Methodology

The system's resilience is based on a calculation of both the value delivery resilience, and the node to node resilience. Once data are collected, assessment of aspects of the system's function, like total information flow, total information flow between nodes, number of node interconnections, traffic demand on a link and on a node, and link capacity can be made. Coupled with an information degradation coefficient applied at nodes and for links, the calculation of resilience can be made. Omer *et al.*[24p.296–300] provide formulae to express these measures.

For this system, reasonably accurate data on node demand, link capacity and traffic flow are available (Omer *et al.*[24] obtain their data from TeleGeography, a telecommunications market research organisation[6]). Node demand is calculated based on the number of people using the Internet in any one region (where a region, or continent, is considered to be a node in the system). Link capacity is derived from standard information available on the cable capacities of the cables used in the links. Lastly, traffic flow is a relative measure of the number of people using a link at any one time – this is dependent on both internal and external use of web addresses at both ends of a link (*i.e.* in countries connected by a submarine optic fibre cable).

4.2.3 Advantages and disadvantages

Importantly, data for each of the indicators used in this measure of resilience are available, meaning direct calculations of both value delivery resilience and node to node resilience are possible. As such, this measure can be used as an absolute measure of the trans-ocean telecommunication system's resilience. While many modern infrastructures are networked, and fundamentally analogous to the model described in this example, this model focuses on ensuring information flow, and not necessarily on some of the technical aspects of the infrastructure, which also play a fundamental role in bringing resilience to a structure or system. This model assumes that if information flow can be maintained in disturbance, then resilience is assured, but without also examining other aspects of resilience, like those discussed in section 3, a fairly limited picture of the system's holistic resilience can be observed.

In addition, individual calculations of the node demand, link capacity, and traffic flow can be used to highlight criticality in the system, because the system's resilience is influenced by the quality of nodes (countries/continents) and links (between-continent optic fibre cables). Nodes with many connections (*e.g.* North America and Europe) and links that carry a large proportion of the global information traffic (between North America and Europe, or between North America and East Asia) are typically the most critical. By identifying these nodes, the networked model of resilience can be used to determine vulnerability, and highlight where investment in protecting nodes, securing links, or increasing link capacity can increase the whole system's resilience. The analysis can also indicate where substitute links may exist, particularly in high traffic areas, where substitutes may be used to divert traffic from high use links to lower use links, thus increasing the redundancy in the system.

5 Developing a resilience index for Swiss Critical Infrastructure

This report follows directly from the CIP Focus Report No. 8, which explored the benefits and limitations of resilience indices. In that report, the authors highlight the growing interest in resilience of critical infrastructures, and particularly the role resilience should play in critical infrastructure protection. The Swiss *'National Strategy for the Protection of Critical Infrastructures'*[7] highlights that Switzerland should become resilient in relation to CI to prevent large scale and catastrophic failure, and to ensure the extent of damage is limited. The strategy points out that in order to 'become resilient', it is important to have tools available that enable resilience to be assessed. A resilience index, therefore, should support the vision of the Swiss national CIP strategy by permitting the assessment of resilience in CIs over time, and particularly as a way to observe the impact of local, cantonal and federal policies aimed at increasing CI resilience.

That the vision envisages "Switzerland [should become resilient] in relation to critical infrastructure..." has implications for the way resilience is assessed. In the context of this focal report, the notion of CI resilience is interpreted as a national priority, requiring a systematic approach, or one that assesses resilience in a holistic

6 www.telegeography.com

7 Bundesrat (2012), *Nationale Strategie zum Schutz Kritischer Infrastrukturen, Bern, 27. Juni 2012,* www.infraprotection.ch

manner. In this case, several considerations specific to the definition of CI resilience outlined in the national CIP strategy must be made. Considering the following issues will be useful in the development of a resilience index for Swiss critical infrastructures.

Establishing strong reasoning behind why it is necessary to assess resilience

This consideration is closely connected to the prioritization of resilience as a necessary feature of Swiss critical infrastructure. As highlighted in this report, there are many reasons why managers of critical infrastructure may want to know whether their asset exhibits resilience in relation to disturbance or shock. Clearly articulating these reasons (*e.g.* because they provide critical services, in order to properly maintain them, to allocate resources for protection, to mitigate vulnerabilities, *etc.*) will assist the definition of pertinent indicators, help to identify stakeholders that should be involved in the process, and determine whether a relative or an absolute measure of resilience is appropriate.

Developing a valid indicator selection approach by engaging relevant stakeholders

Taking a systemic approach to resilience assessment first requires an articulation of the components within a system (the Swiss CIP Inventory, measure 1 of the National Strategy). This process could be well-informed by appropriate stakeholders, who should be engaged in a discussion about the composition of the resilience index given their technical and organisation knowledge of infrastructure operation, maintenance and management. In this context, those stakeholders developing the resilience index must ensure that the indicators chosen reflect what they are intended to measure, based on both the definition of resilience, and the reasoning behind assessing it. This may require testing, or indicator validation processes.

In identifying indicator components of infrastructure resilience, it will also be important to explore how components are related to one another. This is particularly the case if a composite index will be developed. Understanding whether components are inter-related and whether the relationships build or erode resilience will be important to understand the outcome of assessment at the systemic resilience level.

Developing an appropriate methodology to collect data

The methodology for collecting resilience data will be dependent on both the types of indicators being used, and on the overall goal of resilience assessment. Indicators may be quantitative or qualitative (e.g., quality of information transfer), absolute (e.g., speed of CI failure) or relative (e.g., recovery/loss ratio). Quantitative resilience indicators might be most appropriate for technical features of infrastructure, while qualitative indicators may be most appropriate when examining the quality of infrastructure organisation, operation, maintenance or management, or when assessing users' (those who benefit from the service provided by the infrastructure) interactions with infrastructure. This technical/organisational distinction between indicators may also influence whether absolute or relative assessments can or should be made. Technical features of infrastructure are often strongly tangible and therefore directly quantifiable so that characteristics can be measured absolutely (as in the case of the trans-oceanic telecommunications infrastructure resilience detailed in section 4.2). Qualitative features of the infrastructure system are less tangible and more abstract, and identifying direct measures for these is almost impossible (indeed, this is the reason why vulnerability and resilience are assessed using indices). For these, relational assessment techniques are more appropriate, and while not exact, nevertheless provide a comparative means of assessing differences between similar infrastructures, and in observing change in infrastructure characteristics through time.

Establishing how the results of the resilience assessment should be used in practice and/or in policy.

Lastly, effort should be directed towards articulating how the assessment of resilience will be used. Assessing resilience is clearly a very practical goal, yet whether the results are used to inform how an infrastructure should be made more resilient, or as a resilience policy support tool (for example to inform legislation about the use or maintenance of the infrastructure), may determine decisions about why, what, how resilience should be assessed, and who should conduct the assessment.

6 Conclusion

Ultimately, establishing a means to assess CI resilience is an important step toward better decision support in the management of critical infrastructure. As such, resilience assessment processes and methodologies must be dynamic and responsive: to adapt to changing vulnerabilities (through time and with a changing risk environment), but also to changing political imperatives. Although only a small number of resilience indices have been developed in the context of critical infrastructure, their variety (including the two articulated in section 4) highlights how multi-faceted and time-consuming an exercise developing a resilience index is. Although a very practical exercise, the process should be well-informed, well-intentioned and well resourced. It should entail multi-disciplinary and multi-stakeholder deliberation.

Yet the development of a resilience index is not merely a practical problem, it is also a theoretical one that must be supported by basic research. What is resilience? Does the resilience of different infrastructures look different? Will these differences have implications for the method of assessment? How do networks work? How do different infrastructure interdependencies influence resilience? These questions, and many others, are yet to be answered (or resolved), so a program of resilience assessment should be complemented by a strong program of applied resilience research that focuses on technical, social and organisational aspects of resilience. Modern infrastructure is inherently complex. Whether or not complexity confers or detracts from resilience is a question that can be answered by dissociating the components of an infrastructure or its management and assessing how well these components contribute to resilience.

Considerations about critical infrastructure often focus on the technical aspects of the infrastructure (the power connections, the water pipes, the roads and bridges, the cables and telegraph poles, *etc.*). However, while these technical features are fundamental to the infrastructure, and ensure it works, the purpose of critical infrastructure is to provide a service to society. These services are what society most values about critical infrastructure. Clearly, it is important to assess the resilience of the technical features of the infrastructure, but it may also be important to combine these assessments with information about how society values the service provided by the infrastructure – and to incorporate assessments of the infrastructure's social value into considerations about how the resilience of infrastructure (and therefore the continuity of service) might influence policy and practices associated with the infrastructure. This is secondary to developing a useful and meaningful means of assessing infrastructure resilience.

7 References

1. Davidson DJ. The Applicability of the Concept of Resilience to Social Systems: Some Sources of Optimism and Nagging Doubts. Society & Natural Resources. 2010; 23(12): 1135–49. doi: 10.1080/08941921003652940.
2. Holling CS. Understanding the complexity of economic, ecological, and social systems. Ecosystems. 2001; 4(5): 390–405.
3. Liu J, Dietz T, Carpenter SR, Alberti M, Folke C, Moran E, et al. Complexity of coupled human and natural systems. Science. 2007; 317(5844): 1513–6.
4. Ulieru M. Design for resilience of networked critical infrastructures. Digital EcoSystems and Technologies Conference, 21–23 Feb. 2007, Cairns, Australia. DOI: 10.1109/DEST.2007.372035.
5. Klein RJT, Nicholls RJ, Thomalla F. Resilience to natural hazards: How useful is this concept? Environmental Hazards. 2003; 5(1–2): 35–45.
6. Strunz S. Is conceptual vagueness an asset? Arguments from philosophy of science applied to the concept of resilience. Ecological Economics. 2012. doi: 10.1016/j.ecolecon.2012.02.012.
7. Zhou H, Wang J, Wan J, Jia H. Resilience to natural hazards: A geographic perspective. Natural Hazards. 2010; 53(1): 21–41.
8. Birkmann J. Risk and vulnerability indicators at different scales. Applicability, usefulness and policy implications. Environmental Hazards. 2007; 7(1): 20–31.
9. Bara C, Brönnimann G. Resilience – Trends in Policy and Research. Zurich, Switzerland: Center for Security Studies (CSS), ETH Zürich, 2011. Focal Report 6: Risk Analysis.
10. Suter M. Resilience and Risk Management in Critical Infrastructure Protection Policy: Exploring the Relationship and Comparing its Use. Zurich: Center for Security Studies (CSS), ETH Zürich, 2011, Focal Report 7: SKI.
11. Prior T, Hagmann J. Measuring Resilience: Benefits and Limitations of Resilience Indices. Center for Security Studies: ETH Zürich, 2012 Contract No.: Focal Report 8: SKI.
12. Petit F, Collins M, Fisher RE. An index to analyze resilience of critical infrastructure. Arlington, VA 2011.
13. Lonergan S, Gustavson K, Carter B. The index of human insecurity. AVISO (Ottawa, Ont). 2000(6): 1–7.
14. Cutter SL, Burton CG, Emrich CT. Disaster Resilience Indicators for Benchmarking Baseline Conditions. Journal of Homeland Security and Emergency Management. 2010; 7(1). doi: DOI: 10.2202/1547-7355.1732.
15. Tierney K, Bruneau M. Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. TR News. 2007; 250(May–June): 14–7.
16. Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, et al. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra. 2003; 19: 733.
17. Little RG, editor. Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems. System Sciences, 2003 Proceedings of the 36th Annual Hawaii International Conference on; 2003: IEEE.
18. Attoh-Okine NO, Cooper AT, Mensah SA. Formulation of Resilience Index of Urban Infrastructure Using Belief Functions. Systems Journal, IEEE. 2009; 3(2): 147–53.
19. Henry D, Emmanuel Ramirez-Marquez J. Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering & System Safety. 2012; 99(0): 114–22. doi: *http://dx.doi.org/10.1016/j.ress.2011.09.002*.
20. Petit F, Buehring W, Whitfield R, Fisher R, Collins M. Protective measures and vulnerability indices for the enhanced critical infrastructure protection programme. International Journal of Critical Infrastructures. 2011; 7(3): 200–19.
21. Prior T, Hagmann J. Measuring Resilience: Benefits and Limitations of Resilience Indices. Zurich, March 2012: Center for Security Studies, ETHZ, 2012, SKI Focus Report 8.
22. Hagmann J. Risiko, Verwundbarkeit, Resilienz: Neue Gefahrenkonzepte in der internationalen Sicherheitsanalyse. ETH Zürich: Center for Security Studies, 2012. Risk Analysis Factsheet 7.
23. Fisher R, Bassett G, Buehring W, Collins M, Dickinson D, Eaton L, et al. Constructing a resilience index for the enhanced critical Infrastructure Protection Program. Argonne National Laboratory (ANL), 2010.
24. Omer M, Nilchiani R, Mostashari A. Measuring the resilience of the trans-oceanic telecommunication cable system. Systems Journal, IEEE. 2009; 3(3): 295–303.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching, and consultancy and operates the International Relations and Security Network (ISN). The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.