

Enhanced Information Management in Inter-organisational Planning for Critical Infrastructure Protection: Case and Framework

Christine Große^{a}

Department of Information Systems and Technology, Mid Sweden University, Holmgatan 10, Sundsvall, Sweden

Keywords: Information Management, Information Assessment, Analytical Framework, Inter-organisational Information Sharing, Critical Infrastructure Protection, Multi-level Planning, Emergency Response Planning, *STYREL*.


Abstract: This paper develops an analytical framework to assess information in planning for critical infrastructure protection (CIP). Critical infrastructure concerns various societal functions that ensure the daily life, endurance and progress of societies. Thus, CIP involves a considerable number of actors in a multi-level planning that relies on inter-organisational information sharing. Based on a Swedish case of CIP, this study aims to foster information assessment and management that bridge the inherent conflicts between information sharing and information security in CIP. Analyses of the information alongside the Swedish *STYREL* process first exemplify crucial deficiencies in the inter-organisational, national emergency response planning and then specify a set of dimensions and attributes as baseline for assessing information and information processing in CIP. Four stages in the Swedish approach cause a filtering and altering of information that affect the quality of decisions alongside the process and the emergency response plan that relies on them. By assessing the information basis in this large-scale approach, the paper contributes evidence-based foundations for information management in inter-organisational settings, such as the multi-level planning for CIP.

1 INTRODUCTION

Information is an essential prerequisite for planning and decision-making. Alongside multi-level planning processes for protecting vital societal functions and the dependent society, the management of information must maintain an adequate level of information security during acquisition, storage, processing, sharing, utilisation and archiving (European Union, 2008; 2016a). The protection and maintainance of infrastructure that is critical to society's functionality, survival and progression (Cohen, 2010) involves sensitive information and a considerable number of public and private actors in a multi-level socio-technical system-of-systems (Gheorghe et al., 2006). Critical infrastructure protection (CIP) can thus be viewed as a common, societal concern that is located between governmental control and competitive market dynamics as well as the private sphere of citizens (Große, 2020), which includes inter-organisational collaboration and information management. During the course of inter-organisational planning for CIP, the quality of the

processed information is constantly influenced by various requirements, such as the needs of involved decision-makers, the demands of national and international information security policies and the expectations of the diverse actors who are concerned with CIP and crisis management. Since CIP involves secret information about sensitive systems and protection measurements that a nation or business applies, the presence of concrete proceedings in the literature is very limited, such as a discussion of Canada's CIP (Quigley, 2013) and the Swedish approach (Große and Olausson, 2019). Therefore, this study aims to fill this gap and foster information management that bridge inherent conflicts between information sharing and information security in CIP.

Subsequent to the background and method sections, Section 4 presents the Swedish case of *STYREL* and exemplifies crucial deficiencies in this inter-organisational emergency response planning. By analysing the information and information sharing in the currently applied approach, Section 5 provides an analytical framework to assess information in planning for CIP. A conclusion completes the study.

^a <https://orcid.org/0000-0003-4869-5094>

2 BACKGROUND

2.1 Critical Infrastructure Protection

Modern societies increasingly depend on a variety of resources, societal functions and fixed installations, (inter-)organisational structures and agreements as well as legal regulations. Critical infrastructure (CI) concerns a subset of this socio-technical system-of-system, namely, those elements that are critical to society's functionality, survival and progression (Cohen, 2010). Thereby, the energy sector – and the power supply in particular – appears central to this complex system (Rinaldi et al., 2001). Thus, the protection of such infrastructure has gained significance for national security in many countries and for research in this area (e.g. Birkmann et al., 2016; BMI 2009; European Commission, 2004; Große, 2020; MSB 2011), whereas information security is a recurring concern. To protect CI and maintain it during disturbances, such as electrical power failures, national emergency response planning relies on comprehensive information processing. However, the sensitivity of information about CI and the protection measurements that are applied challenges inter-organisational co-operation as well as empirical research in this area (Große et al., 2019). Studies have more often focussed on the operational level of infrastructure, such as the reliability of power transmission (Alvehag and Söder, 2011; Münzberg et al., 2014) and power system restoration (Barsali et al., 2008; Soman et al., 2015; Tortos and Terzija, 2012). By applying a purely technical perspective, such studies ignore not only any societal effects of CI failures but also the interdependencies with public risk and crisis management. However, CIP concerns also the preclusion of unauthorised access to (remote) control systems and the prevention of unauthorised disclosure, altering or loss of sensitive information that is processed and shared.

2.2 Information Management – Quality, Security and Preservation

Information is an essential prerequisite for planning and decision-making. To fulfil its dedicated function of assisting a decision-maker with a decision, information must meet criteria regarding its quality and security. In the context of CIP, such demands can affect each other, which may lead to a paradox that affects the result of a planning process. Information quality is a significant property that is difficult to define and largely depends on the processing of

information through an information system (Michnik and Lo, 2009). In a study with data consumers, Wang and Strong (1996) have captured 118 data quality attributes, which they fused into 20 dimensions and grouped into four higher-level categories. Even though the spectrum of quality attributes remains considerable (Arazy et al., 2017), studies on information quality have successfully reduced the number of categories and identified accuracy, consistency, security, timeliness and completeness as the most common characteristics (cf. Knight and Burn, 2005). For the present study, the information quality dimension adapts the common attributes of intrinsic, contextual and representational information quality, with a particular focus on accuracy, objectivity, timeliness, completeness, format and comprehensibility of information (see Table 1).

In view of the particular significance of information security in the CIP context, attributes that relate to security fit into the information security dimension. Apart from quality attributes, such as accessibility and reputation of the source (Wang & Strong, 1996), the information security dimension in this study includes concerns about the processing of information by a system. Common properties of information security are the availability, integrity and confidentiality of information as well as the privacy of individuals (Andress, 2014, 6–8; 95–99; Independent Data Protection Authorities of the Bund and the Länder, 2016; 2018). Such properties are maintained, to a certain extent, during the processing of information by an information system, whose organisation consists of technical components, formal rules and informal structures with certain information paths. This system influences the quality and security of the processed information (Große, 2016; Michnik & Lo, 2009). In accordance with national and international requirements for national and European CIP (European Union, 2008; 2016a), an adequate level of information security must be maintained during information processing alongside a multi-level planning process for protecting CI and the dependent society (Große, 2018a).

A multi-level planning for CIP, such as the *STYREL* approach in Sweden, depends on not only an adequate level of information quality and security but also the preservation of information. The present study separates this dimension from the former two to emphasise the importance of information preservation for decision-making at subsequent levels of the planning process. Thus, it mainly focuses on the preservation of information, which may exceed archival and technocratic approaches (cf. Quisbert et al., 2009). Of particular relevance to operationalise

the information preservation dimension are the attributes of meaning, as recorded and transferred through the entire process, and evidence of parallel actions (ibid.). These attributes are noteworthy for two reasons. First, they inform evidence-based and rational decision-making through a multi-level and multi-agency planning process (Bharosa et al., 2010). Second, they support sufficient quality and information security management, which is obligatory for national agencies in Sweden (MSB, 2016) to enhance CIP, particularly in the energy and transport sectors (European Union, 2008). Table 1 summarises the conceptual framework that this study applies and briefly explains each attribute.

Table 1: Attributes of Information Quality, Security and Preservation (adapted from: Knight & Burn, 2005; Wang & Strong, 1996).

<i>Dimension</i>	<i>Attribute</i>	<i>Extent to which the information is ...</i>
Information Quality	Accuracy	correct, flawless and certified to be free of error.
	Objectivity	unbiased, unprejudiced and impartial.
	Timeliness / Currency	sufficiently up to date for the task at hand.
	Completeness	of sufficient breadth, depth and scope.
	Format	well organised, concise and consistently represented.
	Comprehensibility	easily understood, interpretable and readable.
Information Security	Availability / Access	accessible for authorised persons at the proper time, in the right place and with the correct degree of access permission.
	Integrity / Reputation	highly regarded in terms of source or content, verifiable, well documented and free of unauthorised alteration.
	Confidentiality	protected from disclosure by unauthorised persons.
Information Preservation	Privacy	limited to a purpose and controllable during a process.
	Meaning	beneficial, undivided and completely transferred.
	Evidence	well documented and completely recorded and transferred.

3 METHODOLOGICAL PROCEEDINGS

This study relies on data and evidence collected from several sources, such as publicly available documents regarding the case, interviews and a survey.

First, the document study examined Swedish documentation of the case; this included handbooks (EA, 2014), guidelines, legal regulations and various reports, (e.g. CAB Blekinge, 2009; CAB Dalarna, 2009; CAB Stockholm 2012; EA, 2012; Veibäck et al., 2013). This examination provided a further basis for the interviews.

Second, interviews were conducted with 66 decision-makers who act on behalf of several actors in this multi-level CIP planning. Table 2 details the participant sample.

Table 2: Participation in the Study.

<i>Number of Interviewees</i>	<i>Affiliation</i>
4	County Administrative Board (CAB)
47	Municipality
15	Power Grid Operator (PGO)

The majority of informants participated in face-to-face interviews within their particular working places. The interviews were semi-structured in nature and consisted of predetermined, open-ended questions, which allowed for a similar structure in each interview while still enabling participants to address any particularly relevant issue with regard to inter-organisational information sharing during the *STYREL* planning. The interviews lasted for an average of one hour, were recorded and transcribed.

Third, to broaden the view of particular issues, the completing survey encompassed all 21 counties in the first step and, in the second step, considered the 10 PGOs that stabilise the power grid during the initial phase of a power shortage. The survey posed 34 questions about the respondents' perceptions of the proceedings of *STYREL* in general and the inter-organisational co-operation and information processing in particular. This proceeding enriched the evidence from the document and interview studies and facilitated a differentiated understanding of the information management in the Swedish process.

The following section describes and analyses the information acquisition, processing and sharing in *STYREL* in detail. Four stages in the planning for CIP cause a filtering and altering of information that affect both the decisions in the process and the resulting emergency response plan. These stages exemplify crucial deficiencies in the inter-organisational, national emergency response planning approach.

4 THE SWEDISH *STYREL* CASE

4.1 Inter-organisational CIP Planning

In 1995, a governmental investigation had already identified the power supply as a critical sector for national security and development in Sweden and discovered a change in threats as well as an increased vulnerability of CI (SOU 1995:19). However, the compilation of a ranking of power consumers to prioritise during such events was not encouraged until after the 2003 blackout in Sweden and Denmark, which may have been the catalyst for the development of the national *STYREL* planning approach (Elkraft System, 2003; Larsson and Danell, 2006; Larsson and Ek, 2004; Svenska Kraftnät, 2003). Since 2004, the Swedish Energy Agency (EA) has been responsible for the development of *STYREL*, which is an acronym for ‘steering electricity to prioritised power consumers’ (EA 2014).

The *STYREL* approach was developed between 2004 and 2011 and executed as a pilot in 2009 and in full-scale in 2010/2011 and 2014/2015 (EA 2014). The third iteration was scheduled to run between 2019 and 2021; however, it is adjourned for one year due to the global SARS-CoV-2 pandemic (EA 2020).

The planning involves many actors from the public and private spheres, including a large number of national agencies and all CABs, municipalities and PGOs (Große, 2017; 2018b). The first two rounds of planning were executed over a period of more than one year and applied a four-year interval. The next planning process will run over a period of three years. Table 3 presents an eight-point scale that the actors in *STYREL* apply as the decision-making aid to identify and prioritise CI in their part of the process.

Table 3: Classification Scheme of CI (MSB, 2010:10).

Class	Score	Description of electricity consumers that have/represent...
1	7	significant impact on life and health—short-term (hours)
2	6	significant impact on society's functionality—short-term (hours)
3	5	significant impact on life and health—long-term (days)
4	4	significant impact on society's functionality—long-term (days)
5	3	significant economic value
6	2	significant importance for the environment
7	1	significant importance for social and cultural values
8	0	Others

As the governmentally entrusted actor, the EA starts the multi-level planning process. Subsequently, the procedure and *inter-organisational information sharing* are suggested as follows (EA 2014):

1. National agencies, which also include CABs to a certain extent, identify and prioritise the CI that each of them operates by applying an eight-digit scale to classify CI (see Table 3).
 - A. Each agency sends one portion of ranked objects to each CAB (up to 21 in total) whose regional area of responsibility the CI object belongs.
 2. Each CAB merges the received lists of prioritised CI and divides them into portions that correspond to each municipality’s area of responsibility.
 - B. Each CAB forwards these lists to each municipality in their region.
 3. Each municipality generates an inventory of local CI and prioritises the objects in accordance with the list in Table 3, which also involves the objects that it receives from the CAB.
 - C. Each municipality sends a request for further information about the prioritised CI to each locally operating PGO.
 4. Each PGO matches the CI objects to power grid areas and power lines within the geographical area in which each PGO operates the local grid.
 - D. Each PGO provides information about technical feasibility of control to each municipality that has sent a request.
 5. Each municipality consequently merges the CI objects into controllable power lines. The spreadsheet in use performs an additive aggregation of the objects’ ranking scores, which yields a ranking list of the power lines. Each municipality is encouraged to assess this list to ensure that the order of power lines reflects the desired position of the particular municipality.
 - E. Each municipality sends the latter list back to the CAB of its region.
 6. Each CAB then combines these lists from the municipalities in its jurisdiction, resolves conflicts between lines that cross municipal or regional borders and finally determines the ranking of power lines.
 - F. Each CAB sends the final document, which contains the ranking of the local power lines in the region, to the national PGO and dedicates portions of it to each provider who operates the local power grid in the region.
 7. Each PGO plans for a manual load shedding within its area of responsibility based on the results of *STYREL* to protect power lines that supply CI from early disconnection.
 - G. Each PGO sends its plan to the national PGO.

4.2 Critical Information Deficiencies

The design of the information flows and processing alongside the multi-level approach of *STYREL* exhibits built-in deficiencies in the information basis necessary for proper decision-making. Several challenges, such as information scarcity in criticality assessments, information withhold in sharing, information loss when sharing and ad-hoc information creation due to scarcity, confront the interorganisational co-operation during *STYREL*. Analyses of the process – both the reference process described in the official documentations and the recent execution of the national process in 2014/2015 – have revealed four critical stages in the process wherein the deficiencies manifest.

1. Identification and prioritisation of CI objects
2. Aggregation (I) of CI objects into power lines at the local level
3. Aggregation (II) of all local power lines to a regional ranking at the regional level
4. Aggregation (III) of regional rankings of local power lines and planning of manual load shedding at the power grid level

The following subsections detail the effects of information deficiencies with regard to the dimensions of information quality, security and preservation (see Table 1) in the Swedish approach of CIP against power shortages.

4.2.1 Identification and Prioritisation of CI

The first critical stage covers the limits during the identification of CI that issue information scarcity in subsequent criticality assessments. The mentioned actors act separately and focus on their portion of CI, which promotes an overvaluation of the CI's criticality within the actor's area of responsibility. The interviews indicate that such overvaluation has occurred at both national agencies and municipalities, which has prompted recurring discussions on the matter. The deficiencies in the information basis at the national, regional and local levels accumulate during the process steps 1 to 3 and manifest in the information-sharing step C, as Section 4.1 describes. The analysis reveals the following issues.

Information Quality

- Underrepresentation of the private sector
- Uncertain whether all CI is present
- Criticality assessment relies on eight-point scale
- Neglects interdependencies between CI/sectors
- Long lists of CI objects

Information Security

- Lack of rules regarding authorised access hampers data collection
- Uncertain how national assets are incorporated
- Fear of disclosure limits integration in risk and crisis management

Information Preservation

- Uncertain whether national prioritisation of local CI objects is preserved
- Uncertain how national and regional CI objects are considered in relation to local CI
- Central management system is absent

4.2.2 Local Aggregation of CI

The second critical stage concerns the aggregation (I) of CI objects into power lines at the local level. The semi-automated aggregation during process step 5 uses an insufficient approach that relies on time-consuming manual control and adjustments. When sharing information during step E, CI information loss is due to the transfer of information from the first spreadsheet to the second one. This transfer affects the granularity of information, which, according to the handbook and the interviews, is motivated by information security concerns as well as recurring discussions of variations in municipalities' interpretations of the priority list (see Table 3). The closer investigation of the local aggregation discovers the following concerns.

Information Quality

- Overly trust in additive aggregation system
- Hardly any reassessment of power lines
- Overwhelming content
- Non-prioritised power consumers are ignored
- No common rules for addressing information gaps

Information Security

- Outdated hardware and software systems affect compatibility and access
- Spreadsheets do not prevent unintended information altering or loss
- Possibility that unrecognised copies exist

Information Preservation

- Irretrievable removal of object information
- Power lines are specified by score, the number of objects in each priority class and a final ranking number
- Rare documentation of assessment and changes

4.2.3 Regional Aggregation of CI

The third critical stage comprises the aggregation (II) of all local power lines to a regional ranking at the regional level during process step 6. According to the information loss at the previous stage, CAB interviewees expressed challenges in generating a regional ranking of power lines from the rankings of up to 49 municipalities. The concerns include manual corrections and further reassessments that necessitate ad-hoc information creation to mitigate the problem of balancing CI's importance between municipalities and regional or national interests. For example, high-priority CI (which may also be of regional or national interest) can fall in the regional ranking if there is a low number of other prioritised CI on that line. Finally, any information on CI is completely lost in the information-sharing step F between CABs and PGOs. Particular emerging aspects are the following.

Information Quality

- Reassessment of power-lines is impossible
- Overwhelming amount of condensed information that each CAB must process
- No common rules for merging the rankings from all municipalities into a county-wide ranking

Information Security

- Variety of hardware and software systems affect compatibility and access
- Uncertain how national and regional CI is represented in the final ranking
- Little knowledge of the source of information
- Unrecognised copies may exist

Information Preservation

- Irretrievable removal of any assessment information
- Power lines are specified by their identifier and ranking number
- No documentation of assessment and changes
- Exchange of experiences in informal networks

4.2.4 Cross-regional Aggregation of CI

The fourth critical stage marks the final aggregation (III) of regional rankings of local power lines and their inclusion in the subsequent planning of manual load shedding at the power grid level. Step 7 of the *STYREL* reference process does not stipulate any approach for this collocation and leaves this decision to the PGOs. In Sweden, there are four power grid areas, 21 counties and 291 municipalities. In one example, the participating PGOs was tasked with

information processing for 120 municipalities and 15 CABs. This PGO bewailed a lack of alternatives and resources to both assess the criticality of the power supply to these lines and update the power supply to CI objects because of information scarcity. The analysis of the information transition to the next-level planning revealed the following deficiencies.

Information Quality

- Reassessment of national, regional or local requirements is impossible
- No common rules for merging the rankings from several counties to a power-area-wide ranking
- No information on contiguous power grids

Information Security

- Different requirements for information security cause manual transfer at PGOs
- Unexpected power line identifiers reveal compromised integrity (between step D and F)
- Altered information can cause inappropriate decisions in emergencies

Information Preservation

- Unclear if the final plan fulfils the goal
- Few PGOs are capable to apply the plan in 15 minutes after order from the national PGO
- About one-third of PGOs did not complete *STYREL* with the manual-load-shedding planning
- Little documentation of proceedings
- Inadequate tracing of changes in the power grid

STYREL applies decentralised processing that lacks a common framework of information security management and quality management. Because of this insufficient system governance, the protection of sensitive information as well as the ability to evaluate the shared content rely on each actor's commitment and effort. The interviews reflect varying perceptions of the significance of these concerns, which may explain why a number of national agencies, such as those concerned with health, post, telecommunication and defence, refrain from participation. However, such withholding of information affects the completeness of information in the planning.

After this examination of the inter-organisational information sharing alongside Swedish emergency response planning for an event of a power shortage, the following section revises the attributes of information quality, security and preservation provided in Table 1. Based on the evidence from the Swedish case, this study discusses and revises each attribute and suggests a framework for the assessment of information and information processing for CIP.

5 INFORMATION ASSESSMENT FRAMEWORK

5.1 Information Dimensions and Attributes in Swedish CIP

Since information is the process object in *STYREL*, the levels of **information quality** at the various stages of the planning influence the quality of the final product, namely the emergency response plan.

Accuracy relates to the correctness of information, such as the identification number of a CI object or the corresponding power line identifier. Accuracy has not always been high in *STYREL*, according to the interviews. Moreover, due to the long planning period in *STYREL* and continuous changes in both the society and the power grid, information which was correct at the point of creation and processing could no longer or not fully reflect societal circumstances once the emergency response plan is finished or must be applied.

Objectivity targets the classification of CI, which should be ascertainable independent of an individual decision-maker. Analysis of the Swedish process illustrates that various interpretations of the classification scheme (see Table 3) have obstructed a uniform assessment of CI. The aggregation of CI objects into power lines and the ranking thereof use a scoring system that promotes objectivity. However, this additive approach does not necessarily reflect the aggregated societal utility of CI objects on a power line. Municipalities and CABs can therefore change the ranking of power lines to achieve a stronger balance between the local and regional ranking of local power lines. These changes in turn can undermine the objectivity of the aggregation (I) approach. The absence of any recommended aggregation method at the regional level (II) and at larger PGOs (III) further weakens the objectivity of this planning process.

Moreover, the interviews have indicated that the second run of *STYREL* mainly used information from the previous planning as the input information, which may raise questions regarding the *timeliness* or *currency* of information. According to interviews with PGPs, the timely extent of the planning process (including the stand-by periods between the process iterations) in combination with grid development and expansion, which have accelerated to meet requirements of renewable electricity production, can eventually challenge the usefulness of the produced emergency plan when it must be applied.

Since the majority of CI is privately operated, the *completeness* of the information basis appeared to be a major problem in *STYREL*. Therefore, it is possible that CI remains unknown as a result of limitations of time, resource allocation and knowledge or the absence of a common set of rules for the dimension in the planning process. For instance, a large part of society is underrepresented in *STYREL*; this includes the private sector and civic society. Security concerns have also prompted national authorities to limit their participation in the planning. Moreover, *STYREL* focuses on electricity-consuming CI objects at the local level, such as buildings. This concentration ignores supply chains and staffing, which can be necessary for the function of an object. In turn, a local object and its services can also be of vital importance for other municipalities or regions, which the *STYREL* approach overlooks.

Issues with the *format* and *comprehensibility* have arisen in Swedish planning from the tools it uses, namely spreadsheets and the classification scheme. These tools require adequate experience to understand and assess the information. The amount of collected information has varied considerably, particularly at the local level. Therefore, municipalities and CABs have employed various strategies to process the content, which include the merging of national assets into the list of local CI. Whereas the local level has information on local CI and addresses the adequate identification of objects and the assessment of each object's criticality for the local society, the regional level lacks object information and thereby faces reduced comprehensibility of information during the task of creating a regional ranking of local power lines. Since the process did not employ a centralised information system, the proceeding further encountered technical issues, such as the compatibility of hardware and software systems, encryption and decryption requirements, and the individual representation on the screen. Interviewees reported that such issues drained their energy, which implies that format and comprehensibility, i.e. proper information *representation*, have a significant effect on the quality of both the processed information and the emergency response in cases of power shortage.

Information security is another vital concern in long-term, large-scale planning. This term encompasses far more than prevention of the disclosure of secrets.

Both the aforementioned tools and further security concerns impeded the *availability* and *access* to information in the Swedish process. First, in 2014/2015, interviewees reported technical issues

due to out-dated software on computers which had no Internet access and which were exclusively used for information processing in *STYREL*. In view of this, it is reasonable to question the availability of collected information at a certain point of time for authorised personnel. Second, since the *STYREL* process does not clarify who is authorised to access which kind of information, some actors withhold information, which can generate a delay in the process and incompleteness of information, for example.

The *reputation of the source* and information *integrity* can support well-documented and verifiable content in CIP planning. In the Swedish case, the majority of interviewees received the classification of CI assets from one national authority that was met with strong rejection of its particular interpretation of the classification scheme. This in turn affected the reputation of the source and led to intended information alteration. Since the recent process lacks feedback loops and evaluation measures, these changes are hardly traceable; thus, a national authority cannot verify whether or to what extent the process includes national assets. In addition, the information processing in *STYREL* can further affect information integrity. For example, the spreadsheets it uses allow for changes – whether intended or not – without recording. Thus, information may have disappeared unnoticed or even by intention.

Since CIP planning concerns the security of a society, the *confidentiality* of concrete CI assets and objects is vital to maintain national security. Although the *STYREL* process does not stipulate any concrete measures to ensure authorised access, the premise is to prevent information from disclosure. The operational realisation rests on the responsibility of each actor and on each CAB in particular due to its double role in the process as a participant and a regional co-ordinator (Große and Olausson, 2018). Observations of the interviewee environment indicate that such proceeding permits a wide spectrum of approaches based on individual commitment and knowledge of information security. Since the lack of common rules, a controllable information-sharing system, and authentication and authorisation measurements in the *STYREL* approach can facilitate information disclosure, the *STYREL* process removes information at each stage which fundamentally affects the information quality for subsequent decision-making.

The information security attribute of *privacy* has gained attention through the implementation of the European regulation on data protection (European Union, 2016b). The majority of CI is privately operated, and businesses that not are legally obligated

to participate in CIP planning can withdraw their participation and require the removal of processed information. In *STYREL*, such removal appears to be an easy task since the information on CI should be stored only at the local level. Nevertheless, the distributed approach of information sharing in *STYREL* makes it almost impossible to assure this case. Local copies may exist with several actors, and the aforementioned copy-and-paste behaviour may cause the re-emergence of information that should have been removed.

The amount and content of information that is processed through and alongside the Swedish process – both formally and informally – requires particular consideration of **information preservation**, as the information that each process step creates and processes acts as input for both subsequent process steps and a later evaluation of the entire process.

On the one hand, the *meaning* of information relates to the individual needs of a decision-maker, both in terms of making sense of the information and perceiving this information as beneficial for the task. During the *STYREL* process, each stage successively reduces the meaning of information by changing, removing and dividing the content. The final ranking at a PGO is a context-free list of numbers and power line identifiers, which does not explain the appearance of such ranking or which reasoning it substantiates. Although the national PGO receives the complete lists from all CABs, the information contains no meaning for this provider at this stage of the process (aggregation II), as the national operator has no knowledge of individual power lines at the regional or local level of the grid. This proceeding constitutes an unnecessary information flow and, thereby, a risk to information security.

On the other hand, information can provide *evidence* of the process and the decisions and actions it involves. However, some respondents remarked that the spreadsheets have minimal space for comments and explanation, and the *STYREL* approach otherwise neither requires nor facilitates any documentation. Few of the respondents reported that they documented the proceeding during the *STYREL* planning in some way, while the majority stated that no other documentation or recording of changes exist. Notably, some could not even identify the location of the produced ranking. The absence of documentation of proceedings by the actors not only elevates the entrance level for new personnel but also precludes a comparison and evaluation of local approaches as well as the entire process.

5.2 Requirements of the Information Basis for CIP

As evidence from the *STYREL* process demonstrates, information management for CIP has to consider several aspects in creating and maintaining an appropriate information basis for decision-making. In the emerging domain of CIP, information quality must compete with information security and information preservation. The triangle of these three dimensions warrants thorough consideration and balance in accordance with the particular needs of a community, society, nation or international co-operation. However, the study also reveals a difficulty in assessing individual, slightly structured approaches that are parts of a whole, large-scale and long-term national process. Particularly, comparisons of local proceedings appeared hardly possible without adequate documentation and criteria for assessment, which in turn hindered an evaluation of consequences of the proceedings for society’s safety. Moreover, no similar cases have been documented in detail from which to learn, and there is not much evidence from larger blackouts or power shortages that could inform information management and development, which relates to such national planning of CIP measures.

This study emphasises several attributes of the three dimensions of information quality, security and preservation. These attributes are commonly used (Arazy et al., 2017; Knight & Burn, 2005), so evidence from the represented case highlights issues that interconnect with these attributes. To enable assessment of local, regional, national or international approaches to information processing in CIP planning, the results of this study can concretise these attributes in the context of CIP (see Table 4).

Table 4: Attributes for Assessing Information and Information Processing in CIP.

<i>Dimension</i>	<i>Attribute</i>	<i>Extend to which the information is ...</i>
Information Quality	Accuracy	correct, flawless and certified free of error at each step and actor in the process.
	Objectivity	unbiased, unprejudiced and impartial regarding the criticality classification of CI assets for a depending society.
	Timeliness / Currency	up to date and updatable at each step, actor and certain point of time in the process.
	Completeness	of sufficient breath, depth and scope to reflect the structure of the society to be protected.

Information Security	Representation	well-organised, concise and consistent as well as interpretable and readable and considerate of the human ability to analyse big data.
	Availability / Access	accessible for authorised persons at the correct time, in the right place and to the appropriate extent of access permission.
	Integrity / Reputation	highly regarded in terms of source or content, verifiable at each step and actor in both directions of the process, and well documented and free of unauthorised alteration.
	Confidentiality	prevented from disclosure by unauthorised persons alongside the process, between process iterations and within the entire information processing system.
	Privacy	limited to CIP, controllable during its life cycle and removable on demand under consideration of regulatory conditions.
Information Preservation	Meaning	beneficial for the task, valuable for sense-making at each step and actor in the process and comprehensive when auditing proceedings, structures and methods.
	Evidence	well documented and completely recorded at each step and actor in the process and at the meta-level for evaluation and improvement of the process and the process development.

Employing a scale for each attribute to indicate the level of fulfilment can facilitate a further evaluation and comparison of particular proceedings, such as those at the local or regional level in *STYREL*. Thereby, such scale can reflect the maturity of each attribute and improve the capability of the process to produce the intended plan for CIP against power shortages. The results of this study demonstrate that the government initiated national efforts towards CIP, while the private sector mainly operates targeted CI assets yet are hardly included in CIP planning. Thus, appropriate public-private co-operation seems necessary to obtain mature planning processes for local, regional, national and global CIP. In particular, process development in the public sector could learn from maturity models and process performance or capability indicators that are common in business.

6 CONCLUDING REMARKS

This study establishes an analytical framework that is built upon three dimensions and 11 attributes to assess information in inter-organisational planning for CIP. To foster information assessment and management that bridge the inherent conflicts between information sharing and information security in CIP, this paper demonstrates the decision-making process in Swedish CIP for the case of a power shortage. Since previous research has emphasised that both the user and the context in which information is acquired and utilised are significant for assessing processed information (Arazy et al., 2017; Bizer and Cyganiak, 2009; Strong et al., 1997; Wang & Strong, 1996), this study clarifies both the process and the dimensions to assess information. In the Swedish case, the decision-makers in the multi-level process are both creators and users of information, whereas a subsequent planning level employs information from a previous level as input in the national policy-making process.

The results have illuminated crucial deficiencies in inter-organisational emergency preparedness and CIP planning that stem from the complexity of information management in such processes. Since *STYREL* applies decentralised information processing, the reference process regulates neither information security management nor quality management. In particular, a filtering and altering of information that affect the quality of decisions alongside the process and the emergency response plan that relies on them manifest at four stages in the Swedish approach. By tracing the information and decision-making during this large-scale approach, this study contributes evidence-based foundations for information management in inter-organisational settings, such as the multi-level planning for CIP.

This study contributes an assessment framework that specifies a set of dimensions and attributes as baseline for assessing information and information processing in CIP. Furthermore, the framework provides support in identifying the extent to which conflicts occur between dimensions and enables analysis to balance them. This element is particularly relevant for CIP, wherein information security and information sharing are important yet conflicting aspects.

The proposed framework and its attributes require further specification, and future studies in domains beyond power infrastructure may reveal additional attributes. Attributes may also differ according to legal situation. Therefore, future development of a process assessment model for CIP should evaluate the

relevance of each dimension and attribute in relation to the others. Moreover, concrete definitions should describe the maturity levels in detail. To establish auditable conditions for a planning process for CIP, such as *STYREL*, minimal requirements must be specified to determine the lowest acceptable level of each dimension and attribute. The development of such maturity model for CIP processes should further consider (upcoming) legal regulations and emerging international strategies for CIP (Mattioli and Moulinos, 2015). Such framework can provide a tool for internal self-assessment by each actor as well as an external audit by an independent body.

ACKNOWLEDGEMENTS

This study was supported by the Swedish Energy Agency alongside the project: ‘Från myndighet till medborgare och tillbaka: En studie av samverkan och kommunikation inom ramen för Styrel’, which is gratefully acknowledged.

REFERENCES

- Alvehag, K., and Söder, L. (2011). A Reliability Model for Distribution Systems Incorporating Seasonal Variations in Severe Weather. *IEEE Transactions on Power Delivery*, 26(2), 910–919.
- Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2. ed.). *The basics*. Amsterdam: Elsevier/Syngress.
- Arazy, O., Kopak, R., and Hadar, I. (2017). Heuristic Principles and Differential Judgments in the Assessment of Information Quality. *Journal of the Association for Information Systems*, 18(5), 403–432. Retrieved June 12, 2018.
- Barsali, S., Giglioli, R., Poli, D., Sforza, M., Salvati, R., et al. (2008). The restoration of an electric power system: International survey and discussion of possible innovative enhancements for the Italian system. *Electric Power Systems Research*, 78(2), 239–247.
- Bharosa, N., Lee, J., and Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, 12(1), 49–65.
- Birkmann, J., Wenzel, F., Greiving, S., Garschagen, M., Vallée, D., et al. (2016). Extreme Events, Critical Infrastructures, Human Vulnerability and Strategic Planning: Emerging Research Issues. *Journal of Extreme Events*, 03(04), 1650017-(1-25).
- Bizer, C., and Cyganiak, R. (2009). Quality-driven information filtering using the WIQA policy

- framework. *Web Semantics: Science, Services and Agents on the World Wide Web*, 7(1), 1–10.
- BMI (Federal Ministry of the Interior) (BMI) (2009). *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin.
- Cohen, F. (2010). What makes critical infrastructures Critical? *International Journal of Critical Infrastructure Protection*, 3(2), 53–54.
- County Administrative Board (CAB) Blekinge (2009). *Styrel. Slutrapport: Länsförsök Blekinge 2009*. 20090924. Karlskrona.
- County Administrative Board (CAB) Dalarna (2009). *Styrel: Länsförsök Dalarna 09 – Slutrapport*. Borlänge.
- County Administrative Board (CAB) Stockholm (2012). *Styrel i Stockholms län: – planeringsprocessen 2011*. Rapport 2012:12. Stockholm.
- Elkraft System (2003). *Power failure in Eastern Denmark and Southern Sweden on 23 September 2003 Final report on the course of events*. Ballerup.
- European Commission (2004). *Research for a Secure Europe*. Luxembourg: Office for Official Publications of the European Communities.
- European Union (2008). Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*.
- European Union (2016a). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*.
- European Union (2016b). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*.
- Gheorghe, A. V., Weijnen, M., Masera, M., and Bouwmans, I. (2006). Introduction. In A. V. Gheorghe, M. Masera, D. L. Vries, and M. Weijnen (Eds.), *Topics in Safety, Risk, Reliability and Quality: Vol. 9. Critical Infrastructures at Risk. Securing the European Electric Power System* (pp. 1–18). Dordrecht: Springer.
- Große, C. (2016). *Towards an Integrated Framework for Quality and Information Security Management in Small Companies*. Master Thesis, Luleå University of Technology, Luleå.
- Große, C. (2017). Applying Systems Thinking onto Emergency Response Planning: Using Soft Systems Methodology to Structure a National Act in Sweden. In *Proceedings of the 6th International Conference on Operations Research and Enterprise Systems (ICORES)* (pp. 288–297). SCITEPRESS.
- Große, C. (2018a). Sources of uncertainty in Swedish emergency response planning. *Journal of Risk Research*, 22 (6), 758–772.
- Große, C. (2018b). The Systemic Implications of Emergent Strategic Objectives in Complex Planning Situations. In *Proceedings of the 7th International Conference on Operations Research and Enterprise Systems (ICORES)* (pp. 287–296). SCITEPRESS.
- Große, C. (2020). *Towards Systemic Governance of Critical Infrastructure Protection: State and Relevance of a Swedish Case*. Doctoral dissertation 325. Sundsvall: Mittuniversitetet.
- Große, C., and Olausson, P. M. (2018). Swedish multi-level planning system for critical infrastructure protection: The regional core. In S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, J. E. Vinnem, & J.-E. Vinnem (Eds.), *Safety and Reliability - Safe Societies in a Changing World. Proceedings of ESREL 2018* (pp. 1893–1901). Boca Raton, FL: CRC Press.
- Große, C., and Olausson, P. M. (2019). Blind spots in interaction between actors in Swedish planning for critical infrastructure protection. *Safety Science*, 118, 424–434.
- Große, C., Olausson, P. M., and Wallman-Lundåsen, S. (2019). Blackout Ahead: Methodological Concerns in Studies of Critical Infrastructure Protection. In M. Beer & E. Zio (Eds.), *Proceedings of the 29th European Safety and Reliability Conference (ESREL)* (pp. 1715–1723). Singapore: Research Publishing Services.
- Independent Data Protection Authorities of the Bund and the Länder (2016). *The Standard Data Protection Model: A concept for inspection and consultation on the basis of unified protection goals*. Kühlungsborn: 92. Conference.
- Independent Data Protection Authorities of the Bund and the Länder (2018). *The Standard Data Protection Model: A concept for inspection and consultation on the basis of unified protection goals*. Düsseldorf: 95. Conference.
- Knight, S.-a., and Burn, J. (2005). Developing a Framework for Assessing Information Quality on the World Wide Web. In InSITE 2005 (Ed.): *InSITE Conference, InSITE 2005* (pp. 159–172). Informing Science Institute.
- Larsson, S., and Ek, E. (2004). The black-out in southern Sweden and eastern Denmark, September 23, 2003. In E. L. Allgower & K. Georg (Eds.): *Vol. 45. Classics in applied mathematics, IEEE Power Engineering Society general meeting*, (pp. 1668–1672). Piscataway, NJ: IEEE Service Center.
- Larsson, S., and Danell, A. (2006). The black-out in southern Sweden and eastern Denmark, September 23, 2003. In (pp. 309–313). Piscataway, NJ: IEEE Service Center.
- Mattioli, R., and Moulinos, K. (2015). *Analysis of ICS-SCADA cyber security maturity levels in critical sectors*. Heraklion: ENISA.
- Michnik, J., and Lo, M.-C. (2009). The assessment of the information quality with the aid of multiple criteria analysis. *Communications of the ACM*, 195(3), 850–856.
- MSB (Swedish Civil Contingencies Agency) (2010). *Styrel - inriktning för prioritering av elanvändare*.
- MSB (Swedish Civil Contingencies Agency) (2011). *Skydd av samhällsviktig verksamhet: DNr 2010-4547*.

- MSB (Swedish Civil Contingencies Agency) (2016). MSBFS 2016-1 Statliga myndigheters informations säkerhet.
- Münzberg, T., Wiens, M., and Schultmann, F. (2014). Dynamic-spatial Vulnerability Assessments: A Methodical Review for Decision Support in Emergency Planning for Power Outages. *Procedia Engineering*, 78, 78–87.
- Quigley, K. (2013). “Man plans, God laughs”: Canada's national strategy for protecting critical infrastructure. *Canadian Public Administration*, 56(1), 142–164.
- Quisbert, H., Korenkova, M., and Hägerfors, A. (2009). Towards a Definition of Digital Information Preservation Object. In M.-A. Sicilia & M. D. Lytras (Eds.), *Metadata and Semantics* (pp. 11–22). New York: Springer.
- Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.
- Soman, S., Thomas, P., George, J., and M, G. (2015). Prevention of blackout by an effective forced islanding and restoration scheme. In *Int. Conf. Emerg. Res. in Electronics, Computer Science and Technology (ICERECT)* (pp. 298–303).
- SOU (Statens offentliga utredningar (SOU) (1995). Hot och riskutredningen: Ett säkrare samhälle. (19.
- Strong, D. M., Lee, Y. W., and Wang, R. Y. (1997). Data quality in context. *Communications of the ACM*, 40(5), 103–110.
- Swedish Energy Agency (EA) (2012). *Slutrapport från Energimyndighetens styrel-projekt: ER 2012:04.*
- Swedish Energy Agency (EA) (2014). *Styrel: Handbok för styrels planeringsomgång 2014–2015.* ET2013:23,
- Swedish Energy Agency (EA) (2020). *Information angående ändring av tidplan för styrelplaneringen.* 2018-006963.
- Svenska Kraftnät (2003). *Elavbrottet i södra Sverige och i östra Danmark 2003-09-23: Preliminär rapport om händelseförloppet som ledde till avbrottet.*
- Tortos, J. Q., and Terzija, V. (2012). Controlled islanding strategy considering power system restoration constraints. In IEEE (Ed.), *Power & Energy Soc. Gen. Meet. New Energy Horizons - Opportunities and Challenges* (pp. 1–8).
- Wang, R. Y., and Strong, D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems*, 12(4), 5–33.
- Veibäck, E., Stenérus Dover, A.-S., Fischer, G., and Lindgren, J. (2013). *Elnätsföretagens MFK-planering: En studie av elnätsföretagens möjligheter att genomföra manuell förbrukningsfrånkoppling baserad på Styrel.* FOI-R--3797--SE. FOI.