Critical infrastructure resilience: A Nordic model in the making?[1]

ABSTRACT
In recent years, there has been a shift in emphasis from critical infrastructure protection to that of resilience. This development reflects the acknowledgment that complete protection can never be guaranteed, and that achieving the desired level of protection is not cost-effective as a rule in relation to the actual threats. This article reviews the responses of four of the five Nordic countries to this challenge, namely Denmark, Finland, Norway and Sweden. The article analyzes their strategies and conceptual development, highlighting the common trends and differences. In so doing, it argues that these countries have a better starting point for the task of making their critical infrastructure resilient than most of the EU. This is due to the fact that even before the resilience debate emerged, these countries had based their policies on securing vital societal functions rather than the individual infrastructures that support these functions. The article concludes that some kind of Nordic model can really be identified when it comes to approaches towards critical infrastructure resilience. It should also be recognized, however, that there has been a fruitful interplay at the conceptual level between the Nordic countries and the EU that has inspired and influenced both parties.

Keywords:
Critical infrastructure
Resilience
Civil protection
Crisis management
Nordic model

1. Introduction

The notion of the Nordic model is well-known is such fields as national economic and social policies that contribute to the welfare state, which combines free market capitalism with rather heavy state regulation and re-distribution policies. But is there a Nordic model, compared to the rest of the European Union (EU), or the European Commission-sponsored (EC) approaches, when it comes to critical infrastructure (CI) resilience in the context of more generic civil protection approaches?

Although there are five Nordic countries, this article only analyzes Denmark, Finland, Norway and Sweden (leaving Iceland aside), suggesting that these four constitute a reasonably representative sample of the Nordic region. While only Denmark, Finland and Sweden are EU members, Norway is closely connected to the Union through its membership of the European Economic Area (EEA), and in practice often follows the same policies as the EU in the field of

[1] This article is a by-product of the IMPROVER project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390.

civil protection. However, fundamentally, in spite of the EU's efforts to coordinate efforts for civil protection and critical infrastructure protection (CIP), especially in such cases when this infrastructure can be understood as European Critical Infrastructure (ECI), at the end of the day critical infrastructure remains the sole responsibility of the member states.

2. Methodology

The current analysis focuses on the conceptual and programmatic developments of the EU and the four Nordic countries respectively, rather than any empirical and sector-specific case studies. This comparative approach is applied to several dimensions of the puzzle. First, the developments are compared across changes over time, ranging from the early 2000s to the contemporary situation, in order to identify general trends. Second, the Nordic countries are viewed from the perspective of wider developments in the EU, thereby comparing their developments vis-à-vis the EC policies. Third, when reviewing the four Nordic countries, the account also explicitly becomes a comparative study of each one. Finally, the review is organized in terms of five sub-areas or binary test questions, as illustrated in Table 1.

Table 1
Comparative methodology (Table 1 also in a separate attachment)

Country/area	Critical infrastructure or vital societal functions?	Protection or resilience?	Terrorism or all-hazards approach?	National or macro-regional resilience?	Regulation or public-private partnership?
EU	General characteristics and trends				
Denmark					
Finland					
Norway					
Sweden					

Section 3 provides a rather descriptive review of these five test questions, discussed somewhat more analytically in section 4. The results of this comparative exercise are summarized in the concluding section 5 and its accompanying Table 2.

3. Comparative review

In accordance with Table 1, each part of this review section starts with more generic notions about international or EU approaches, followed by concise reviews of the respective Nordic countries' positions. More emphasis is put on the similarities rather than country-specific idiosyncrasies – which obviously reflect each country's traditions, location, challenges and experiences, administrative-political systems, and so on – although some specific differences are highlighted. The main sources of evidence are official documents, namely those major statements, policy papers, strategies and so forth that should be seen as constitutive of more specific and even operative actions.

3.1 Critical infrastructure or vital societal functions?

After 9/11, the concept of CIP became a new catchword in the US [1, 2, 3]. It quickly caught on in Europe as well, first through NATO and then within the EU soon thereafter. After the 2004 Madrid and 2005 London terrorist attacks, the EU debate culminated in the development of the European Programme for Critical Infrastructure Protection (EPCIP) and its corresponding legislation [4]. The EU Directive from 2008 [5] defines critical infrastructure as follows: "An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".

In 2012 the EPCIP was reviewed by the EC [6], and a degree of self-appraisal is apparent in the working document that ensued. The review states that a number of member states follow "system-focused national CIP programmes where the end goal is security and resilience of systems, which may involve activities across multiple sectors". While the member states referred to in this statement are not identified in the document, it is clear that this description can readily be applied to the Nordic countries, including non-EU-member Norway. To this end, the Nordic countries were not merely passive adopters of the EU approach but, on the contrary, influenced future EU policies with their own approach.

Even before the resilience discourse emerged in the context of critical infrastructure, it was clear that the CIP terminology and definitions used by the Nordic countries adhered to their own longer-term traditions, and the solutions they had adopted to meet new circumstances.

In other words, the Nordic CI concept was based on the traditional total defence or civil defence systems that were built up during the Cold War. 'Total defence' usually refers to the need to take all defence dimensions into account, including military, economic, civil, social, and psychological defence. In the Finnish context, for instance, this is usually referred to as 'comprehensive national defence' today: "The preparedness of Finnish society is executed with the principle of comprehensive security, which entails the safeguarding of vital functions of society in a joint effort of the authorities, the business sector and organisations and citizens". [7]

By definition, this approach then becomes a more inter-sectoral and more resilience-oriented starting point – compared to mere CIP policies – from which to develop current strategies. Based in part on this Cold War experience and the constant uncertainty which characterized that era, all of the Nordic countries also have well-developed redundancy and storage-based systems to secure the supply chain of critical materials and services, such as energy and basic public health-related drugs.

In any case, the Nordic countries speak more about critical or vital societal functions than mere CI. In Denmark, for instance, its 'National Risk Profile' is based on vital societal functions. In the 2013 National Risk Profile [8], prepared by the Danish Emergency Management Agency (DEMA) and subordinated to the Ministry of Defence, the agency refers to activities, commodities, services, and so forth that underpin society's general ability to function. The 2017 version of the National Risk Profile [9] in turn offers a 'consequence model' for each threat scenario, divided into six levels. From the 'bottom up' these comprise societal functions; property; economy; environment; health; and life. Hence, the fundaments entail societal functions rather than individual infrastructures.

Finland never abandoned the Cold War total defence approach, but rather developed it further amid new conditions. Finland's first CIP approach from 2006 was titled 'The Strategy for Securing the Functions Vital to Society' [10], which reveals even more clearly than the Danish document that the approach focuses on vital societal functions rather than the infrastructures that support them. The main emphasis is on the functioning of society and government in all circumstances, not only protecting its individual critical infrastructures against extreme events.

In a similar vein, the early Swedish model from 2007 was called ‘Critical Societal Functions’ [11]. The whole spirit of the Swedish approach was, like Finland’s, more about resilience than mere protection. However, the Swedish model differs from the Finnish one to some extent by putting much more emphasis on local rather than national government-level functions, reflecting the two countries’ somewhat different administrative systems and political culture.

An important feature of the Swedish definition is that societal functions that are critical in emergencies can vary from situation to situation. It is not possible to list all of the functions that are critical for society in every situation, which is why it is important to analyze the specific societal functions that are critical in different situations. This approach is basically what the more analytical literature calls the consequence-oriented definition of criticality, whereby it is less the infrastructures themselves that are critical but more the criticality of the consequences of infrastructure failure [12].

In one sense, Norway’s early CIP system was a synthesis of many approaches. Like its Nordic neighbours, Norway also chose to speak about critical or vital societal functions rather than just critical infrastructure. In the Norwegian approach – called ‘Protection of Critical Infrastructures and Critical Societal Functions in Norway’ [13] – both the concept of infrastructure and that of function were included as elements at different levels. Critical societal functions formed a more general level, being dependent on but also encompassing infrastructures. The hierarchical idea was that society’s basic needs are covered by critical societal functions, which depend on infrastructures, whose criticality is assessed according to three criteria: dependability, in that a high degree of dependability implies criticality; alternatives, in that few or no alternatives imply criticality; and tight coupling, in that a high degree of tight coupling or linkage within a network implies criticality. This approach forms the basis for deciding whether any given infrastructure is critical or not. In practice, the approach makes it possible to limit the extent of the CI considerably, because not every part of, say, an electricity grid or a transport system is necessarily considered critical, which is the case in the EU approach at the conceptual level.

In a 2017 report by the Norwegian Directorate for Civil Protection (DSB), titled ‘Vital functions in society. What functional capabilities must society maintain at all times?’ [14], the term ‘vital societal functions’ is defined and the functions are listed and categorized. The term is reserved for “functions that society could not cope without for seven days or less without this threatening the safety and/or security of the population”. The term is further divided into three broad categories: governability and sovereignty; security of the population; and societal functionality. Listed under these categories are the functional areas and assets that are usually brought up in critical infrastructure discussions, such as the government and other administrative bodies, the emergency services, essential utilities such as energy and water, and so forth. It is noteworthy that the very term ‘critical infrastructure’ is not mentioned at all, with the term ‘infrastructure-based services’ being used instead.

3.2 Protection or resilience?

When EPCIP, the European Programme for Critical Infrastructure Protection, was launched, the concept of resilience did not appear in policy documents. While the ‘Green Paper’ [15] that introduced EPCIP recognizes that not all infrastructures can be protected against all threats, its solution was to prioritize the protective measures in relation to each other and then to focus on selected protected objects. Similarly, the subsequent Council Directive on EPCIP [5] is characterized by the same approach and, consequently, by the absence of any reference to resilience.

Although the concept of resilience has deep roots in many disciplines, in its contemporary meaning it may be appropriate to trace it back to the ecological debates of the early 1970s [16]. The concept was popularized in unofficial policy and scientific analyses in the mid-2000s in the context of crisis and disaster management. Before long, it also entered the academic field of critical infrastructure studies, replacing the earlier focus on protection [17, 18, 19]. After some years, this paradigm shift became visible at the policy level as well, first and foremost in the US [20]. As was the case with the concept of CIP, the EU followed the same trajectory after lagging behind for some years. In the 2012 Commission review of EPCIP [6], the concept of resilience already plays a role, albeit a small one. As an alternative concept to protection, resilience didn’t start to appear in the EC institutions in earnest until about 2014 [21].

What then is the difference between protection and resilience? The Council Directive on EPCIP [5] defines protection as “all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability". On the other hand, no official EU definition has been suggested as yet that would be suitable for CI purposes in particular. However, a generic definition, also applicable to CI, is provided by the United Nation's International Strategy for Disaster Reduction (UNISDR) [22], namely: "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions". At national levels, however, several definitions of resilience exist [23], more or less following the UNISDR definition above.

It is notable in the UNISDR definition that the verb 'resist' implies that protective measures are included. Resilience can thus be understood as an umbrella concept that also covers CIP. Hence, in our scheme it basically covers all the 'phases' of the traditional crisis management cycle. Resilience focuses on preventive, mitigative and preparedness activities before the crisis hits, as well as the response during the crisis. Most notably, it also deals with recovery after the crisis, in the event of the disruption of a CI service, for example.

The exact boundaries of the resilience discourse in the context of CI are still rather blurred. Nevertheless, certain sub-discourses have emerged, and have even become institutionalized. Consequently, we can differentiate between at least three separate, albeit partially overlapping domains of CI resilience: societal, organizational, and technological. When defining the resilience domain, in principle we can approach the issue from the perspective of the organizations or institutions that are in charge of taking the appropriate actions before, during or after a harmful and unwanted event affecting CI service provision.

In *societal* resilience, the important actors are national and local governments, communities and households, and it is in these contexts that critical infrastructure resilience often overlaps with normal civil protection or crisis management efforts. In *organizational* resilience, the actors are businesses, especially those responsible for critical infrastructures and supply chains. In *technological* resilience, the actors include critical infrastructure and the respective facility operators, and, to some extent, safety and security manufacturers and vendors [21, 24].

As for the Nordic countries, resilience has implicitly been present from the very emergence of their CIP policies, precisely because they concentrated not only on sectoral infrastructures, but also on vital societal functions. However, even if resilience does happen to be the main term when discussing safety and security issues in the Nordic countries at present, it is only fairly recently that it has been applied and concretized into CI in particular.

Denmark has a well-developed societal safety and security system, coupled with the respective research activities. However, when it comes to resilience or CI resilience, the subject is not yet well argued. The country's vulnerability analyses from 2005 to 2010 [e.g. 25, 26, 27] prepared by DEMA, the Danish Emergency Management Agency, hardly touch upon the concept of resilience, focusing instead on vulnerability as the inverse concept. Thus, the 2006 vulnerability analysis can be quoted as stating that "vulnerability (and its opposite, resilience) expresses a given system's general ability to function and achieve its goals when faced with threats. A system is vulnerable when it lacks or has reduced capacity to plan for, prevent, respond to or recover from a realized threat. Vulnerability assessment is carried out comparing threats against existing capacities, as well as the preferred degree of protection".

In this approach, the concepts of vulnerability and resilience seem to be two sides of the same coin, effectively sharing the same definition, while resilience per se is not discussed separately. However, the term resilience is covered indirectly in that the official documents use words like robustness, vulnerability and recovery, which can be seen as key words or elements in the concept of resilience. The 2013 'National Risk Profile' [8], for instance, mentions in the introduction that society must be robust and prepared for accidents and disasters. In the latest 2017 National Risk Profile [9], resilience is not mentioned at all, but the analysis model is based on an application of the typical crisis management cycle with its pre-, during, and post-crisis phases, and can thus be seen as essentially including all the elements of resilience. However, the main focus is perhaps on protection (or the prevention, preparedness and respond phases) rather than on resilience in terms of rapid recovery. The DEMA report from 2015 on the country's crisis management system [28], for instance, states that the purpose is "to ensure a robust society by developing and strengthening preparedness, in order to prevent and respond to major accidents and disasters".

Similarly, in the case of Finland, the concept of resilience has only recently progressed from academic discussion into official policy documents. In Finland's 2016 'National Risk Assessment' [29], the concept, in its translated form, already plays a rather prominent role. The Finnish-language equivalent, which could perhaps be expressed as 'crisis withstandness', emphasizes rather clearly that although it is not possible to prevent every crisis, one still has to build up resilience to persevere and recover from the materialized crisis quickly. The concept of crisis resilience is even included in the Government's 2016 'Foreign and Security Policy Report'[30], reflecting its connection with the traditional total defence concept.

In Norway, too, resilience as such is a rather new concept, especially when it comes to CI, even if it might have been implicitly present earlier. Viewed more holistically, after the major terrorist attacks in Oslo and on Utøya Island on July 22, 2011, the Ministry of Justice and Public Security released a report to the Norwegian Parliament concerning public security, approved by the State Council [31]. The concept of resilience does not appear in the report, however. Nor does the Royal Decree of 2012 [32], which focuses on the same subject, use that term. However, both reports mention CI. The Royal Decree stresses that the departments are to evaluate risks, vulnerability and robustness vis-à-vis critical infrastructure within their own sector, on the basis of the Norwegian Directorate for Civil Protection (DSB) national risk analysis. Further, the resolution states that different departments should consider carrying out preventive and preparedness-related measures to strengthen the robustness of critical infrastructure and important societal functions. Even more attuned to the spirit of resilience, the evaluation should include the ability to maintain or recover important societal functions under the strain that an unwanted event would entail. In sum, all the key elements of CI resilience can be found in this document, yet without using the concept of resilience itself as an explicit umbrella term.

The 'National Risk Analysis', prepared by the DSB in 2013 and updated in 2014 [33, 34], already takes the concept of resilience on board, although basically only its societal domain, to the exclusion of the organizational or technological domains. It states that "resilient societies" is a relatively new concept in civil protection. However, the report emphasizes that the concept is becoming increasingly important, stressing that due to the complex relationships and mutual interdependencies in society, resilience may become of even greater strategic importance in the future in terms of efforts to strengthen civil protection. As a source of conceptual inspiration, the report refers to the World Economic Forum's *Global Risks 2013* [35] as a strategy for continuously identifying new hazards and threats through risk analyses and the preparation of plans to meet these risks. This is said to be a strategy for confronting events of which we have little knowledge and no prior intelligence of their probability or consequences. The DSB report goes on to state, using the definition by Norris et al. [36], that resilient societies are characterized by being able to adapt to changing conditions during and after extraordinary stress and strain. “The properties that characterize resilient societies are robustness, redundancy and the ability to respond rapidly.” In the concluding remarks, the report highlights that the less that is known and the greater the uncertainty about a type of risk, the more obvious resilience becomes as a strategy.

Sweden was definitely one of the first countries to make the societal safety and security approach more about resilience than mere protection [37]. In 2011, commissioned by the Swedish Government, the Swedish Civil Contingencies Agency (MSB) published a national strategy for the protection of important public services [38]. In the introduction, it states that the purpose of the strategy is to develop a more resilient society. In that context, resilience is defined as “the capacity the society has to withstand and recover from a disruption”. In 2013, MSB published a report [39] under the title ‘Resilience – the concept’s different meanings and utilization areas’. The report states that its mission is to contribute knowledge about how the term resilience is used across different sectors, rather than suggesting how and where MSB should use the term. Hence, the report provides a number of different definitions from different organizations. Furthermore, it stresses that the term resilience will be subject to further development and that MSB will follow this development. MSB has also decided on a research strategy for 2014 to 2018. The strategy includes, among other things, the goals of protecting important public services, analyzing risk and vulnerability, and enhancing resilience [40]. In 2015, MSB contributed considerable funding to the establishment of the Centre for Critical Infrastructure Protection Research (CenCIP), based in Lund University. While the endeavour failed to emphasize resilience over protection, the practical research is nonetheless largely about the former.

3.3 A terrorism or all-hazards approach?

In the early phases of the CIP debates, especially in the US, the focus was predominantly on terrorism-related threats [41, 42]. This was the case even prior to 9/11. For instance, the US presidential report in 1997 stated that “While poor design, accidents and natural disasters may threaten our infrastructures, we focused primarily on hostile attempts to damage, misuse, or otherwise subvert them" [41]. Naturally, the emphasis on deliberate attacks was hugely reinforced after 9/11. The idea that western states "face a determined, intelligent enemy who seeks to cause us maximum harm", and that the focus should therefore be on worst-case analysis [43], became prevalent in the US. This approach was largely copied by the EU. Terrorist attacks, especially the Madrid 2004 and London 2005 bombings, were actually the catalyst for launching the EPCIP in the first place. The terrorism-as-threat-scenario approach was to some extent mirrored in institutionalized solutions. In the EU, for instance, the EPCIP came to be coordinated by the Directorate General that was responsible for police affairs, rather than the directorate responsible for civil protection. Moreover, NATO's CIP focus was originally on "ways to assist nations in improving their preparedness for the protection of civilian populations from terrorist attacks against critical infrastructure" [42].

The partial revival of the all-hazards approach in the US CI strategy, while retaining terrorism as the main threat, only came about after Hurricane Katrina in 2005, which shifted the focus away from the one-sided emphasis on terrorism somewhat [44]. The EU approach similarly ended up balancing between terrorism and an all-hazards approach. However, in November 2005 when the Commission published the 'Green Paper' [15] that was to be discussed by stakeholders in the member states, it gave three options concerning the threats: an all-hazards approach for everything; an all-hazards approach that prioritized terrorism; and a terrorism hazards approach. If one then looks at the Commission's Directive Proposal of December 2006, a terrorism-as-priority approach was adopted, although reference was also made to the concept of 'threat' defined as "any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof" [45]. The European Parliament wanted to add their amendments that "structurally determined threats should also be covered" but the "threat of terrorism should, however, be given priority" [46]. The final Council Directive refers to an earlier Justice and Home Affairs Council call from December 2005 for the Commission to prepare the EPCIP under an approach, where "man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority" [5].

This approach was obviously at odds with the traditional all-hazards approach of the Nordic countries – even if they also took, and continue to take, terrorism and other malicious threats against CI seriously.

All of the Nordic countries have prepared national risk assessments in recent years – in some cases even several – based on an all-hazards approach. This has been largely, and paradoxically, inspired by the EU, but more recently by those parts of the EC that deal with civil protection rather than CI or police matters. Indeed, there are a considerable number of EU policies contributing to disaster risk management in the all-hazards spirit [47]. One of the most informative in the current context is the Commission document 'Overview of Natural and Man-made Disaster Risks in the EU', the first version of which was published in April 2014 [48]. The document is a summary analysis of the national risk assessments of (at that time) 18 member states and associated countries, prepared by following a joint risk assessment methodology provided by the Commission [49], which in turn was based on the ISO 31000 standard [50].

The April 2014 [48] document starts from the assumption that information provided by national authorities is sufficient for drawing general conclusions about "the most important disaster risks that a large number of Member States are addressing, focusing in particular on risks with a cross-border dimension". The guidelines set by the Commission [49], in turn, state that member states should consider all significant natural and man-made hazards that could occur "on average once or more every 100 years (i.e. annual probability of 1% or more) and for which the consequences represent significant potential impacts, i.e. number of affected people greater than 50, economic and environmental costs above €100 million, and political/social impact considered significant or very serious".

On the basis of the 18 national risk assessments, the document identifies the twelve most addressed hazards as follows: (Natural hazards:) Floods, Severe weather, Wild/Forest fires, Earthquakes, Pandemics/epidemics, Livestock epidemics; (Man-made hazards:) Industrial accidents, Nuclear/radiological accidents; Transport accidents; Loss of critical infrastructure; Cyber attacks; and Terrorist attacks. In one section, the document also discusses emerging risks. These include climate change-related hazards (including migration), space-related hazards (space debris, space weather, near-Earth objects), and anti-microbial resistance.

While all of the above hazards could easily trigger critical infrastructure service disruptions, it is worth noting that the loss of CI is also listed as a separate category. The corresponding section in the document emphasizes the interconnected nature of CI systems, especially energy networks, which rapidly cascade from one country to another. The following countries expressed particular concern about CI losses in their national risk assessments: the Czech Republic, Germany, Ireland, the Netherlands, Poland, Sweden, and the United Kingdom.

Of the Nordic countries, Denmark, Norway, and Sweden are represented in the above-mentioned EU risk assessment summary. Finland subsequently prepared its first national risk assessment in 2016, and Denmark, Norway and Sweden have since updated theirs. Currently, the EU requires each member state to update its risk assessment every three years.

In 2013, the Danish Emergency Management Agency (DEMA) published its first 'National Risk Profile' [8], although it had previously produced so-called vulnerability reports on a regular basis [25, 26, 27] (like the other Nordic countries under different labels). The 2013 report classifies incidents according to whether they are man-made or natural, where natural incidents are divided into extreme weather phenomena and serious contagious diseases, and man-made incidents into two sub-categories: accidents and security threats. DEMA selected ten incident types for further investigation: hurricanes, strong storm and storm surges, heavy rain and cloudburst, pandemic influenza, animal diseases and zoonoses, transport accidents, accidents involving dangerous substances on land, marine pollution accidents, nuclear accidents, terrorist acts, and cyber-attacks.

The latest 'National Risk Profile' from January 2017 [9] in turn divides the risks into event types and tendencies. While all of the above-mentioned risks are mentioned, water and food-borne diseases as well as space weather have been added. Moreover, the tendencies include security policy tensions, antibiotic resistance, irregular migration, and increased activity in the Arctic.

In a separate Danish 'Security Intelligence Risk Assessment' from 2015 [51], the report refers to two sources in terms of the threat landscape: Russia, which "has access to cyber capabilities suited to bolster the country's conventional military operations, such as targeted operations against critical infrastructure", as well as "non-state actors, including ISIL", who engage in cyber efforts to hack critical components, resulting in a system breakdown.

The Finnish ‘National Risk Assessment’ [29] was published in late 2016. On the basis of the assessment of over 60 risks, 21 possible event scenarios for Finland were selected for in-depth discussion. The risks are categorized into two types, namely wide-ranging events affecting society (6 risks) and serious regional events (15 risks). Cyber risks are discussed in some detail under the first category, differentiating between utilizing the cyber domain to paralyze systems vital to society, risks associated with cybercrime, and data security risks in digitalization. This category includes, in addition to the typical nuclear accident risk, a 100-year risk scenario for a solar storm, in line with Norway and Sweden and some other European countries. Most natural disaster risks are considered serious regional events, together with terrorist attacks targeted against Finland. The timing of the Finnish risk assessment also explains why a mass influx of migrants is included as a national risk, unlike the European risk assessments that were prepared two or three years earlier.

Norway has been a part of EU risk assessment efforts, but it had already been active in this field before, independently of the EU coordination. According to the Royal Decree of 24 June 2005, the Norwegian Directorate for Civil Protection was ordered to prepare a vulnerability and preparedness report that would serve as the baseline for further safety and preparedness investigations across sectors and departments [52]. The aforementioned reports have been prepared from 2012 onwards under the name ‘National Risk Analysis’ [33, 34].

Norway’s 2014 ‘National Risk Analysis’ [34] divides hazards into natural events, major accidents and malicious events, where each category is further divided into risk areas with associated scenarios. The six most probable scenarios are all natural events, including extreme weather, forest fires, epidemics, avalanches, and space weather. The risk areas that have the greatest consequences for society, overlapping with the aforementioned, are security policy crises, earthquakes, extreme weather, nuclear accidents, epidemics, cyberspace, and avalanches. The scenarios with the highest risks are then carefully evaluated, and are related to epidemics, earthquakes, nuclear accidents, extreme weather and avalanches. As is apparent, natural events are considered not only more likely but also more risky than man-made malicious risks. A terrorist threat in a big city is one of the scenarios discussed in the report, however. It is mentioned that the threat of terrorism against Norway is regarded as heightened, possibly including the capacity to use chemical, biological, and radiological substances, as well as nuclear material.

In 2011, the Swedish MSB began work on its national risk assessment, as commissioned by the government. In the ‘National Risk Assessment’ published the following year [53], MSB “identified 27 particularly serious national events, which were derived from the more than 200 events identified in the agencies’ risk and vulnerability analyses of 2010–2011”. The report states, however, that MSB does not consider the 27 scenarios analyzed to represent the greatest risks facing Sweden as a country. Instead, they should be viewed as in-depth studies of a selection of events that were considered to be particularly serious in the risk identification phase. Among the 27 events were incidents such as disruption of the fuel, food and electricity supply, the flooding of water sources, a contaminated drinking water supply, heatwaves, pandemics, landslides, storms, and so on. Added to this, eleven scenarios were developed, while seven were analyzed and assessed. Of these events, a school shooting and a prolonged heatwave were deemed the most likely to occur. A major fire on a cruise ship, disruption of the food supply due to fuel shortages, and the failure of a large dam on a river were evaluated to have the greatest impact. The events entailing the greatest overall risk in terms of a combination of likelihood and severity were a fuel shortage leading to a disrupted food supply, the failure of a large dam on a river, and a prolonged heatwave.

In 2016, MSB published an updated version of the national risk assessment [54]. This already comprises a rather comprehensive collection of risk assessments, together with a capability assessment. The risks are categorized into four main groups: natural hazards (10 different risks), major accidents (4), disruption to technical infrastructure and supply systems (7), and antagonistic hazards (4). The third category plainly concerns critical infrastructure, and includes the following categories: disruptions to the energy supply; disruption to electronic communications; disruption to the payment system; disruption to the food supply; disruption to the drinking water supply; disruptions to the transport system; and disruption to the supply of drugs. Cyber-attacks and terrorism are listed under antagonistic hazards. Resilience is mentioned only in passing in this document, noting that critical infrastructure should be made robust and resilient in order to avoid severe cascading effects.

3.4 National or macro-regional resilience?

It is clear that the ability to identify and analyze interdependencies is an important part of CI resilience. Although interdependencies are a common feature of critical infrastructure systems, often materialized via cyber connections through information and communication technology, many of them are regionally determined in that they are closely related to geographical proximity, geographical functionality, and integrated regional networks. This is particularly true in the Baltic Sea Region and especially in the Nordic countries, where critical infrastructures are in many sectors part of the very same Nordic infrastructure system. This concerns highly physical infrastructure such as electricity grids, as well as less physical infrastructure such as financial and banking services. It is useful, therefore, to take into account the particular regional cross-border effects of critical infrastructure vulnerabilities as well as the specific features of European sub-regions [37], more often referred to as macro-regions in EU parlance today.

Contrary to expectations, the EU framework, namely the EPCIP Directive of 2008 [5], has proved ineffective as a means of enhancing cross-border or macro-regional cooperation. In practice, that part of the CI within two sectors – energy and transport – that is designated as European critical infrastructure (ECI) has to be nominated by a member state, and its identity remains undisclosed. Very few member states have exercised this right as they do not wish to be regulated. Among those who have, some close-to-border CI, such as power stations or grids that provide services across borders have been nominated. According to the EPCIP Directive [5], this entails producing a preparedness plan in line with a specific EC template. As these infrastructures are not only rather randomly selected or nominated, but also remain undisclosed as a rule, even within the EC, the visible impact of the EPCIP is very low. What remains is for the EC to provide some kind of support for national CI.

The Nordic countries are known for their close cooperation, however, which is traditionally deeper and has a longer pedigree than EU cooperation. The main fora for this have been the Nordic institutions, particularly the Nordic Council of Ministers (NCM), which coordinates intergovernmental cooperation between the countries. In the field of safety and security, this cooperation focuses on civil protection rather than critical infrastructure or its resilience, but these fields naturally overlap. The first Nordic framework agreement in the field of rescue cooperation dates back to 1989 between Denmark and Norway; Finland and Sweden joined in 1992, and Iceland in 2001. This cooperation, encompassing highly practical and operative cross-border arrangements, is called NORDRED. Since 2005, civil protection has been included at a wider and higher level within NCM’s cooperation areas. In practice, this entails high-level ministerial or Director General-level meetings twice a year with some preparatory committees. At this level, the result may be a common statement, like the Haga Declaration from 2009 and the Haga II Declaration from 2013, issued by the Nordic ministers for civil protection, which called for the Nordic countries to adopt the same strategic approach across borders in the Nordic region. This high-level mandate in turn has provided the impetus for regular, rotating crisis decision-making workshops and training, as well as projects focusing on cross-border crisis-management issues.

A major project in this context revealed that rather widespread bottom-up, albeit fragmented, cooperation already existed, even at the regulatory level; the project detected 76 cross-border rescue cooperation agreements within the Nordic area. One of the challenges has consequently been to enhance the coordination of this cooperation in order to gain a holistic picture of its features [55]. At a more concrete level, several full-scale exercises are held on a rather regular basis with the participation of all or most of the Nordic countries in order to enhance interoperability, often organized within the EU Civil Protection context and with the assistance of respective funding.

Another cooperation forum is the Council of the Baltic Sea States (CBSS), which includes all of the Nordic countries plus the three Baltic States, Germany, Poland and Russia, as well as the European Commission, represented by the European External Action Service (EEAS). Civil protection cooperation in terms of Director General meetings, civil servant cooperation and macro-regional projects has existed since the early 2000s, the latter often with EC funding. This cooperation intensified after the adoption of the European Union Strategy for the Baltic Sea Region (EUSBSR) by the European Council in 2009. This is the first macro-regional strategy in Europe, and it is organized into several policy areas (PA), one of which is EUBSR PA Secure, including both civil protection as well as law enforcement cooperation. This cooperation is coordinated by the CBSS and the Swedish MSB. While the EUSBSR as such is based on existing funding, it greatly facilitates the macro-regional cooperation on safety and security. Several past, current and planned projects in this context focus on risk assessment and risk management, gap and capacity analysis, and on enhancing resilience [56, 57].

3.5 Regulation or public-private partnership?

So where do private actors fit into the picture? This is an important question when it comes to CI in particular. Governments are usually legally responsible for safeguarding CI, and yet most of it is owned, administered and operated by the private sector. This is why public-private partnership (PPP) is regarded as a major issue in safeguarding national infrastructure [58]. While in the US private industry traditionally owns most of what is defined as national infrastructure, its share being estimated at 85 per cent, in many European countries infrastructures such as water, energy, and railway transportation have previously been the sole remit of the government. However, ever since the 1980s, these infrastructures have been undergoing a process of market liberalization and privatization. The rapid development of the predominantly privately owned and operated information and communication technology (ICT) sector, and other sectors' dependence on it, has complicated the situation. This, coupled with other critical infrastructure interdependencies, has led to a rather ambiguous situation in terms of the real authority, as government authorities may have, either formally or informally, overall responsibility for the reliable provision of services, but they lack the authority, resources and skills to actually fulfil that responsibility [18]. Hence, private industry is supposed to be able to exert extensive self-regulation because, in practice, only they have access to the necessary technical capabilities and information pertaining to most of the CI.

Added to this, globalization, with its tendency to move private companies outside the nation state, has made the situation more complex from the perspective of government control. The fact that national CI are dependent not only on other sectors but on the situation in other countries complicates the situation because no single country is either immune to the effects, or able to predict the outcomes, if its neighbours suffer from serious infrastructure disruptions [59].

Here we face the dilemma of the common good. Some have proposed that the solution lies in the concept and practice of Corporate Social Responsibility (CSR): “The link between CSR and critical infrastructure resilience is a compelling argument to understand and advance the social role for corporations in business” [60]. However, while CSR and PPP may seem self-evident and are celebrated by all parties, this shallow consensus is usually broken when it becomes clear that governments expect the private sector to make considerable investments beyond their cost-benefit calculations. Thus this dilemma leaves governments with only two options: to provide the necessary resources itself, funded out of the public budget, or to increase regulation [18].

In the US, the approach is clearly based on voluntary private sector cooperation with the federal government. This is largely due to the country's anti-regulation traditions, and the private sector's willingness to do their share precisely in order to avoid regulation. Compared with the US, the EU approach, referring to national rather than EU legislation, seems to mark a step towards regulative efforts instead of mere voluntary compliance, although both the US and the EU put emphasis on the importance of PPP [21].

None of the Nordic countries has thus far arrived at any clear solution to this dilemma. Undeniably, CI operators usually do prepare all kinds of regulatory and voluntary risk assessments, but the regulation is rather light, and often outdated. In Finland's 'National Risk Assessment' this issue is highlighted in the case of cyber threats in particular. It states that critical infrastructure in Finland is for the most part owned by the private sector and companies tend to follow commercial logic, "which creates a challenge for cyber security preparedness". The report also states that legislation "does not take a uniform approach to cyber threats. Rather, legislation in this field is sector-specific. It is also a challenge to discern between an attack against an individual actor – a crime – and an act against the state". Furthermore, the report concludes that "whereas cyber threats carried out by states are typically cross-border threats, the powers of national authorities only apply inside their sovereign borders" [29].

There is, of course, rather detailed regulation in all countries related in particular to so-called high-risk industries, such as nuclear power plants, as well as organizations connected to critical public services, such as hospitals. They should have updated risk assessments as well as the respective capacities and capabilities, which are monitored in principle by certain independent state or municipal agencies. In many privately-owned CI cases, however, this regulation is also rather vague from the perspective of resilience.

Adding regulation would force the private sector to invest more resources in dealing with the protection or resilience of the systems they own or operate. This would be an unwelcome change for many CI operators because markets are externalizing CI risks at present, whereas state regulation would mean establishing "liability rules based on the notion that organizations should internalize the costs of the risks they produce and that by internalizing them, they will make wiser choices about the technologies they use" [12]. This in essence would necessitate a well-functioning tort liability legislation, which would make it easy for consumers, both public and private, to subsequently demand compensation for losses incurred by critical infrastructure failures, which in turn would force industry to pay more pre-emptive attention to security and protection out of self-interest.

In terms of the classification of resilience into societal, organizational and technological domains, one can say that while the first is largely covered by the actions of national and local authorities, or even partially by communities and households, the two latter domains are the responsibility of the CI operators. At least in the literature, it is possible to identify a normative tendency to recommend moving from typical risk management towards resilience management. This is motivated by the fact that risk assessment, being a part of risk management, reveals only the preventive, mitigating and preparedness efforts that are needed to treat risks before a crisis, whereas resilience management also covers the during-the-crisis and after-the-crisis phases. In this sense, resilience management would be close to what is usually understood as crisis management – or the crisis management cycle [61].

But how should resilience management be carried out? While in the field of risk management one can find more or less popular and authorized standard frameworks, most notably the ISO 31000 standard [34], there are no standards when it comes to performing resilience management. How do we know whether a CI is resilient or not? Can resilience be measured? How can it be enhanced? In fact, a number of models do exist, some of which are only theoretical applications while others are already in operational use [24, 63, 64], and designed for CI resilience assessment. No such models are in operative use in Europe, however. In order to pave the way for more structured resilience assessment, the EC is currently financing around six projects in its Horizon 2020 programme, which, taken together, are designed to contribute to forthcoming European guidelines for resilience, focusing largely on CI resilience. The Nordic countries, through research institutions but also in association with civil protection authorities as well as CI operators to some extent, are well represented in these projects, which may eventually contribute to CI resilience in such a way as to become firmly established in these countries in more practical terms.

4. Discussion

So what can we glean from the concise review above? Is there a specific Nordic model, and is it one that other countries could learn from?

We have reviewed this issue mainly at the conceptual level, focusing on five issue areas that were formulated as dichotomies. The first issue considered the level of analysis. Should one focus on CI or on vital or critical societal functions instead? From a comparative perspective, the Nordic countries analyzed here, namely Denmark, Finland, Norway and Sweden, have fairly similar conceptions concerning critical infrastructure. They all proceed from a more fundamental level of vital societal functions, which in turn are provided by CI. This is clearly a more inter-sectoral approach compared to the original EPCIP, and closer to the concept of resilience, even if that concept was not yet fashionable when the Nordic approaches were formulated. One can argue that the tradition of the Cold War total defence concept – currently enjoying a revival in the Nordic countries – influenced this more holistic view, at least in Finland and Sweden. The EC, in turn, seems to have been favourably disposed towards this approach, which could well be formulated as a 'Nordic model'.

The second issue was related to how the resilience concept is handled in the Nordic countries' policies. Arguably, the concept of CI resilience has not completely replaced CIP in the Nordic countries, and the debate and conceptual development vis-à-vis resilience mainly focus on society as a whole, rather than on CI, where the emphasis still seems to be on typical risk assessment and risk treatment approaches in terms of preventive and protective measures. However, one can see that the traditions of focusing on vital societal functions and the general attitudes towards safety and security support the development of more detailed and concrete resilience policies and programmes in the near future. At the present time in these countries, one can hardly participate in safety and security debates without bringing up the concept of resilience.

The third issue considered the threat scenarios – whether one should focus on terrorism when it comes to CI, or whether one should adopt an all-hazards approach. The original EPCIP approach clearly emphasized the terrorist threat against CI, somewhat undermining other threats. This might still be the case, and the focus could perhaps be more decidedly on ECBRN (explosive, chemical, biological, radiological and nuclear) threats, rather than all-hazards when it comes to CI.

However, the general EU civil protection approach is clearly an all-hazards one. The national risk assessments of the Nordic countries, following the EC guidelines, were prepared in this spirit. In this field, coordinated by the EC bodies responsible for civil protection rather than CI, all-hazards is the norm. Admittedly, the risk assessments of the respective countries were not prepared simultaneously, let alone in concert, and in spite of the common methodological guidelines provided by the EC [33], the methodologies vary from country to country. However, one can still conclude that the Nordic risk assessments basically identified the same risks. All of the countries rely heavily on an all-hazards approach, and terrorism is not accentuated more than cyber risks, extreme weather, or floods, for instance. This comes as no surprise, given the similar circumstances of the four countries.

One can also refer to the recent Finnish and Swedish assessments in particular, where one can identify a trend of progressing from mere risk assessment towards outlining risk treatment options as well, which would be the logical next step according to the ISO 31000 standard [34]. However, both risk assessments fail to venture very far in this direction. Indeed, they just routinely describe existing actions or institutions vis-à-vis risks (Finland) or capabilities (Sweden) that are already in place, rather than paying systematic attention to a range of generic risk treatment options for each identified risk, in accordance with the ISO 31000 standard.

The fourth issue concerned national approaches versus macro-regional cooperation. While both civil protection and CI remain under the national authority, one can conclude that the macro-regional dimension of cooperation between the Nordic countries, and more widely within the Baltic Sea Region, is producing tangible results in terms of harmonizing or approximating vocabulary and approaches, adopting good practices, organizing exercises, and creating – within the Nordic countries in particular – a legal and regulatory framework for civil protection cooperation. The NCM and the CBSS are crucial facilitators of this cooperation. Nevertheless, it would be difficult to imagine this activity without strong EU support, especially where funding and the supporting framework of the EUSBSR are concerned. While CI resilience is not directly addressed in terms of close cooperation with CI operators, the societal dimension of resilience is, and includes both national competent authorities as well as regional and local actors.

The last issue discussed the problem of how to organize CI resilience efforts, considering that most of the CI is, in fact, owned and operated by profit-making private actors. Should it be handled through regulation or public-private partnership? It can be concluded that the Nordic countries do not have any specific model or solution for this puzzle. Regulation is clearly fragmented and non-coordinated vis-à-vis the so-called new threats in particular, such as cyber security. The cooperation between state authorities and private CI operators is, however, facilitated by dint of the fact that in small countries people in the same field, both civil servants, politicians, private company actors and researchers, tend to know each other and meet regularly in seminars, workshops and committees.

On the other hand, if we look at Nordic CI operators from the perspective of whether they carry out resilience assessments, any random survey reveals that the vast majority is actually performing risk assessment and management, but hardly anyone uses the term resilience, let alone speaks about applying any structured methodology to assess or test it. It seems that the impetus in this field should come from the EC. If some kind of guidelines for CI resilience assessment could be agreed upon at the EU level, this would probably make the concept more widespread for operative use, not only in the Nordic countries but also in Europe at large.

That said, the conceptual review presented above does not paint the whole picture. First, it arguably takes too homogenous a view of the situation. While the approaches look similar, there are some crucial differences in the countries’ civil protection and crisis management systems at the administrative level, reflecting their general political-administrative systems that vary in many respects [64, 65]. Second, a conceptual analysis does not say much about practice. While any country obviously handles crises with varying degrees of success, it is difficult to test the existence of a resilient system from a comparative perspective. Some crisis management studies, however, do suggest that there are differences in practice in the way that the Nordic countries have managed the same crisis situation [66].

5. Conclusions

It is clear that the concept of CI resilience (perhaps to be called CIR in the future) is gradually replacing the original CIP, with the latter focusing on protective measures and resilience as opposed to focusing on the whole cycle of a crisis, emphasizing the impossibility of safeguarding against all threats. The current analysis has discussed the puzzle of whether there is any specific Nordic model with regard to CI resilience in particular, taking the wider issues of civil protection on board as well. The comparative perspective has been applied at many levels: across time, between the EU approach and the Nordic approaches, and between the Nordic countries of Denmark, Finland, Norway and Sweden. The puzzle was also scrutinized in more detail through five issue areas or crucial ‘test questions’, reviewed in section 3 and briefly discussed in section 4. The results of this investigation are summarized in Table 2.

Table 2
The Nordic model vs. the EU model (Table 2 also in a separate attachment)

Country/area	**Critical infrastructure or vital societal functions?**	**Critical infrastructure protection or resilience?**	**Terrorism or all-hazards approach?**	**National or macro-regional resilience?**	**Regulation or public-private partnership?**
EU	Originally based on sectors that were identified as critical, such as transport and energy.	Originally based only on protection; since 2012 the term resilience has started to play a more important role.	Originally the focus within critical infrastructure was on terrorism, although an all-hazards approach has gradually entered the picture from the civil protection field.	Has failed to create a European approach as such in critical infrastructure (unlike in civil protection). Yet supports national efforts in protection and resilience efforts concerning critical infrastructure. The EUSBR approach facilitates civil protection cooperation.	Encourages national regulation.

Denmark **Finland** **Norway** **Sweden**	Early emphasis on vital societal functions rather than on critical infrastructure only.	Implicit emphasis on resilience. The concept is still rather new, with a focus on societal resilience.	Clear all-hazards approach from an early stage.	Substantial Nordic and Baltic Sea States cooperation, but not so much in the field of critical infrastructure to date.	Unclear national regulative framework. Some public-private partnership cooperation in the field of critical infrastructure. Critical infrastructure operators carry out sophisticated risk assessment and management, but no explicit resilience assessment thus far.

Looking at Table 2, it seems that a Nordic model of some description does exist, or is at least 'in the making' when it comes to approaches towards CI resilience, or in any case the conceptual development and basic philosophy appear to be rather similar, taking into account the obvious idiosyncrasies. Even from an early stage, the Nordic countries' approaches have been more holistic than those of the EC, focusing on vital societal functions rather than mere sector-based infrastructures. In the current study of resilience, these countries do not seem to experience any difficulty in moving from CIP to a more resilience-based paradigm. Moreover, they all clearly rely on an all-hazards approach, refraining from putting undue emphasis on the terrorist threat scenario. They are not only engaged in cooperation within the EU, but they have also adopted an institutionalized approach towards cross-border cooperation within the Nordic and Baltic Sea countries.

However, if one accepts the division of resilience into societal, organizational and technological domains, this Nordic approach is more visible in the societal resilience domain, where the national and local authorities are the key players. When it comes to CI operators, the concept of resilience is still rather abstract and lacks concrete operationalization. So, one can argue that the interplay between the authorities and CI operators, be it discussed in terms of regulation, state support, public-private partnership or corporate social responsibility, remains the weak link in achieving CI resilience in practice.

The review of the Nordic countries' conceptual approaches towards CI-related crises nevertheless gives the impression that these countries are rather 'progressive' and have always had a broader and more holistic philosophy than the one originally offered by the EC, based on prioritizing the protection of CI against terrorism. However, this argument can be tempered to a considerable extent by noting that there has been a fruitful interplay at the conceptual level between the Nordic countries and the EC/EU, with each inspiring and influencing the other.

References

[1] Moteff, J. (2003) *Critical infrastructures: background, policy, and implementation*, Report for Congress. Received through the CRS Web, Order Code RL30153, The Library of Congress.

[2] Moteff, J., Copeland, C., and Fischer, J. (2003) *Critical infrastructures: What makes an infrastructure critical?* Report for Congress, Received through the CRS Web, Order Code RL31556, The Library of Congress.

[3] K.A. Brown (2006) *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, Fairfax: Spectrum.

[4] C. Pursiainen (2009) The Challenges for European Critical Infrastructure Protection, *Journal of European Integration*, Issue 31/6 (2009), pp. 721–739.

[5] European Council (2008) *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Council Directive 2008/114/EC of 8 December 2008.

[6] European Commission (2012) *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)*, Brussels, 22 June 2012, SWD(2012) 190 final.

[7] Ministry of Defence of Finland (n.d.) *Comprehensive National Defence* [Online] Available at: http://www.defmin.fi/en/tasks_and_activities/comprehensive_national_defence.

[8] DEMA (2013) *National Risk Profile (NRP)*, The Danish Emergency Management Agency, Denmark, Birkerød.

[9] DEMA (2017) *Nationalt Risikobillede*, Beredskabsstyrelsen, Denmark, Birkerød.

[10] The Government of Finland (2006) *The Strategy for Securing the Functions Vital to Society*, Government Resolution 23 November 2006.

[11] MSB (2017) *Critical Societal Functions*, Swedish Emergency Management Agency, Sweden, Stockholm.

[12] M.J. Egan (2007) Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems, *Contingencies and Crisis Management*, Volume 15 Number 1, March (2007) pp. 4–17.

[13] Justis- og politidepartementet (2006) *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004, Avgitt til Justis- og politidepartementet 5. april 2006, NOU Norges offentlige utredninger 2006: 6. Departementenes servicesenter Informasjonsforvaltning, Norway, Oslo.

[14] DSB (2017) Vital functions in society. What functional capabilities must society maintain at all times? Norwegian Directorate for Civil Protection, Norway, Oslo.

[15] EC (2005), *Green Paper on a European Programme for Critical Infrastructure Protection*, Commission of The European Communities, Brussels, 17 November 2005, Com(2005) 576 Final.

[16] C.S. Holling (1973) Resilience and Stability of Ecological Systems, *Annual Review of Ecology and Systematics*, 4, pp. 1–23.

[17] P.L. Scalingi (2007) Moving beyond critical infrastructure protection to disaster resilience. In: *Critical thinking: Moving from infrastructure protection to disaster resilience*, CIP Program Discussion Paper, School of Law, US, George Mason University, pp. 49–72.

[18] M. De Bruijne and M. Van Eeten (2007) Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment, *Journal of Contingencies and Crisis Management*, Vol. 15, No.1, pp. 18–29.

[19] A. Boin and A. McConnell (2007) Preparing for critical infrastructure breakdowns: The limits of crisis management and the need of resilience, *Contingencies and Crisis Management* 15, (2007), no. 1, pp. 50–59.

[20] J.D. Moteff (2012) *Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress*, Congressional Research Service 7-5700, August 23.

[21] C. Pursiainen and P. Gattinesi (2014) *Towards Testing Critical Infrastructure Resilience*, Publications Office of the European Union, JRC Scientific and Policy Reports, Luxembourg.

[22] UNISDR (n.d.) *Terminology on Disaster Risk Reduction*, United Nations International Strategy for Disaster Reduction, Switzerland, Geneva, [Online] Available at: http://www.unisdr.org/we/inform/terminology.

[23] CIPedia (n.d.) [Online] Available at: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Resilience.

[24] C. Pursiainen et al. (2016), Critical Infrastructure Resilience Index. In: L. Walls, M. Revie and T. Bedford (eds.), *Risk, Reliability and Safety. Innovating Theory and Practice*, Boca Raton, CRC Press, pp. 2183–2189.

[25] DEMA (2005) *National Sårbarhedsrapport 2006*, Beredskabsstyrelsen, Denmark, Birkerød.

[26] DEMA (2006) *National Sårbarhedsrapport 2008*, Beredskabsstyrelsen, Denmark, Birkerød.

[27] DEMA (2008) *National Sårbarhedsrapport 2008*, Beredskabsstyrelsen, Denmark, Birkerød.

[28] DEMA (2015) *Crisis Management in Denmark*, The Danish Emergency Management Agency, Denmark, Birkerød.

[29] Ministry of the Interior (2016) *Finland National Risk Assessment 2015*, Internal security, Ministry of The Interior Publication 4/2016, Finland, Helsinki.

[30] Valtioneuvoston kanslia (2016) *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko*, Valtioneuvoston kanslian julkaisusarja 7/2016, Finland, Helsinki.

[31] Ministry of Justice and Public Safety (2012) *Samfunnssikkerhet*, Report to the Storting 29 (2011-2012), Norway, Oslo.

[32] DSB (2012) *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap*, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering, Royal Decree of 15 June 2012, Norwegian Directorate for Civil Protection, Norway, Oslo.

[33] DSB (2013) *National Risk Analysis 2013*, The Norwegian Directorate for Civil Protection, Norway, Oslo.

[34] DSB (2014) *National Risk Analysis 2014*, The Norwegian Directorate for Civil Protection, Norway, Oslo.

[35] World Economic Forum (2013) *Global Risks 2013 - Eighth Edition*, World Economic Forum, Switzerland, Geneva.

[36] F.H. Norris et al. (2008) Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *Am J Community Psychol.*, 41(1–2), pp. 127–150.

[37] C. Pursiainen (ed.) (2007) *Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection*, Nordregio Report 2007:5, Sweden, Stockholm.

[38] MSB (2011) *Ett fungerande samhälle i en föränderlig värld: Nationell strategi för skydd av samhällsviktig verksamhet*, Swedish Civil Contingencies Agency, Sweden, Karlstad.

[39] MSB (2013) *Handlingsplan för skydd av samhällsviktig verksamhet*, Swedish Civil Contingencies Agency, Sweden, Karlstad.

[40] MSB (2013) *Resiliens: Begreppets olike betydelser och användsområden*, Swedish Civil Contingencies Agency, Sweden, Karlstad.

[41] President's Commission on Critical Infrastructure Protection Critical Foundations (1997) *Protecting America's Infrastructures*, [Online] Available at: https://fas.org/sgp/library/pccip.pdf.

[42] I. Abele-Wigert, and M. Dunn (2006) *International CIIP Handbook 2006 VOL 1. An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, series editors A. Wenger and V. Mauer (Swiss Federal Institute of Technology Zurich), Switzerland, Zürich.

[43] G.M. Brown et al. (2006) Defending Critical Infrastructure, *Interfaces* Vol. 36, No. 6 (November–December), pp. 530–544.

[44] P. Parfomak (2005) *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, CRS Report for Congress, Received through the CRS Web. Order Code RL33206, The Library of Congress, US, Washington.

[45] EC (2006) Commission of the European Communities, Proposal for a Directive of the Council on Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection, Brussels, 12 December 2006, COM(2006) 787 final.

[46] European Parliament (2007) *P6_TA(2007)0325 European Critical Infrastructure, European Parliament legislative resolution of 10 July 2007 on the proposal for a Council directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*, (COM(2006)0787 – C6-0053/2007 – 2006/0276(CNS).

[47] EC (2014) *EU Policies contributing to Disaster Risk Management*, Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The post-2015 Hyogo Framework for Action: Managing risks to achieve resilience. Commission Staff Working Document, Brussels, 8 April 2014, SWD(2014) 133 final.

[48] EC (2014) *Overview of natural and man-made disaster risks in the EU*, European Commission, Commission Staff Working Document, Brussels, 8 April 2014, SWD(2014) 134 final.

[49] EU (2010) *Risk Assessment and Mapping Guidelines for Disaster Management*, European Commission, Commission Staff Working Paper, Brussels, 21 December 2010, SEC(2010) 1626 final.

[50] ISO (2009) *Risk management – Principles and guidelines, ISO 31000:2009*, International Organization for Standardization.

[51] Danish Defence Intelligence Service (2015) *Intelligence Risk Assessment. An assessment of developments abroad impacting on Danish Security*, Denmark, Copenhagen.

[52] DSB (2005) Royal Decree of 24 June 2005, Ministry of Justice and Public Security, Direktoratet for samfunnsikkerhet og beredskap- det generelle koordingeringsansvaret for

koordinering av tilsyn med aktiviteter, objekter og virksomheter med potensial for store ulykker, The Norwegian Directorate for Civil Protection, Norway, Oslo.

[53] MSB (2016) *Swedish National Risk Assessment 2012*, Swedish Civil Contingencies Agency, Sweden, Karlstad.

[54] MSB (2016) *A summary of risk areas and scenario analyses 2012–2015*, Swedish Civil Contingencies Agency, Sweden, Stockholm.

[55] MSB (2011) *Enhanced cross-border operational cooperation for civil protection in Northern Europe: Results and Recommendations*, Swedish Civil Contingencies Agency, Sweden, Stockholm.

[56] [Online] Available at: http://www.14point3.eu/tasks-2/task-c/.

[57] [Online] Available at: http://www.gapstocaps.eu/.

[58] I. Abele-Wigert (2006) Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspective. In: M. Dunn and V. Mauer (eds.), *International CIIP Handbook, Vol. II. Analyzing Issues, Challenges, and Prospects*, series editors A. Wenger and V. Mauer (Zürich Swiss Federal Institute of Technology Zürich), Switzerland, Zürich, pp. 139–167.

[59] D. Mussington (2002) *Concepts for Enhancing Critical Infrastructure Protection. Relating Y2K to CIP Research and Development*, Prepared for the Office of Science and Technology Policy, RAND Science and Technology Policy Institute, US, Santa Monica, CA.

[60] G. Ridley (2011) National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience, *Journal of Business Ethics* (2011) 103, 111–125.

[61] C. Pursiainen (2017) *The Crisis Management Cycle*, UK: Routledge.

[62] B. Rød et al. (2017) Evaluation of resilience assessment methodologies, in M. Cepin and R. Briš (eds.) *Safety and Reliability – Theory and Applications*, Boca Raton, CRC Press, pp. 1039–1051.

[63] B.E. Biringer, E.D. Vugrin, and D.R. Warren (2013) *Critical Infrastructure System Security and Resiliency*, Boca Raton: CRC Press.

[64] C. Pursiainen, S. Hedin and T. Hellenberg (2005) *Civil Protection Systems in the Baltic Sea Region. Towards integration in civil protection training*, (Eurobaltic Publications 3), Helsinki: Aleksanteri Institute.

[65] T. Christensen et al. (2016) Comparing Coordination Structures for Crisis Management in Six Countries, *Public Administration*, Volume 94, Issue 2, June, pp. 316–332.

[66] A. Brändström, A. Kuipers, and P. Daléus (2008) The politics of tsunami responses: comparing patterns of blame management in Scandinavia. In: A. Boin, A. McConnell, and P. ’t Hart (2008) *Governing after crisis. The politics of investigation, accountability and learning*, Cambridge: Cambridge University Press, pp. 114–147.