
Taylor & Francis
Taylor & Francis Group

Sustainable and Resilient Infrastructure

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tsri20

# From European critical infrastructure protection to the resilience of European critical entities: what does it mean?

Christer Pursiainen & Eero Kytömaa

**To cite this article:** Christer Pursiainen & Eero Kytömaa (2022): From European critical infrastructure protection to the resilience of European critical entities: what does it mean?, Sustainable and Resilient Infrastructure, DOI: 10.1080/23789689.2022.2128562

**To link to this article:** https://doi.org/10.1080/23789689.2022.2128562



Published online: 03 Oct 2022.

SUSTAINABLE AND RESILIENT INFRASTRUCTURE
https://doi.org/10.1080/23789689.2022.2128562

Taylor & Francis
Taylor & Francis Group



# From European critical infrastructure protection to the resilience of European critical entities: what does it mean?

Christer Pursiainen [a] and Eero Kytömaa [b]

[a]Faculty of Technology and Science, Department of Technology and Safety, UiT the Arctic University of Norway, Norway; [b]National Security Unit, The Ministry of the Interior, Finland

**ABSTRACT**

The article is a public policy analysis of the development of legislation on critical infrastructure in the European Union (EU), covering 27 developed countries. More precisely, it concerns the 2022 CER Directive "on the resilience of critical entities'. This directive replaced the 2008 ECI Directive 'on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection'. We ask what is at stake in this process of moving from one directive to another. Why has the concept of protection been replaced by the concept of resilience, and why has the concept of critical infrastructure been replaced by the newly invented euro-concept of 'critical entity'? In the concluding section we discuss the European integration dimension of this new directive; what does this development in the CI domain tell us about the current dynamics of European integration, and how it could be explained?

**ARTICLE HISTORY**
Received 19 August 2022
Accepted 15 September 2022

**KEYWORDS**
Critical infrastructure; resilience; European Union policymaking; creeping integration

This is a public policy analysis of the development of the European Union (EU) legislation on critical infrastructure (CI), highlighting its change, promises and challenges. The issue is of obvious importance for the 27 member states of the EU, all developed high-technology market economies and often with interconnected CI. However, the issues arising from this perspective are also of interest to countries outside the EU as all the countries have to tackle the same challenges: how to enhance the resilience of CI and thereby also the resilience of the societies in which they are embedded.

The issue is complex and multifaceted. On the one hand, it is about the very issue area of CI, with all its dimensions, sectors, actors, and so forth, and particularly the concept of resilience in this context. On the other hand, it delves into the very issue of European integration itself. The question concerns how the relationship between the member states and the EU evolves even in such a field that basically belongs to the member states' mandate. The CER Directive testifies to further integration beyond the already supranational areas in the EU.

While CI was traditionally outside of supranational regulation in the EU, this started to change around fifteen years ago. In 2008, the so-called ECI Directive (Council of the European Union, 2008) 'on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection' became the first binding European Union regulation in the respective field. It paved the way for a new area of European integration. In December 2020, the European Commission (2020a), based on several mid-term reports and a rather comprehensive public stakeholder hearing process, published its proposal to replace the ECI Directive with a new one, known as the CER Directive 'on the resilience of critical entities'. This new directive was finally approved in 2022.

The EU system, with all its governance bodies, is rather complex. To make it more comprehensible, one often says, metaphorically speaking, that the European Parliament (representing nationally selected party politicians) is a kind of lower house. The European Council (representing the heads of government or heads of state who define the general political direction and priorities), together with the Council of the European Union (representing the line ministers of member states in different policy areas) comprises the upper house or senate. The European Commission then is the initiating and executive government in areas of common policy. As the EU directive procedure goes, also in our case (see Figure 1), the European Commission made the proposal in 2020, then six issue-area committees of the European Parliament duly discussed it and gave their detailed opinions. The amendments proposed by the committees reveal more about the

**CONTACT** Christer Pursiainen christer.h.pursiainen@uit.no

attention paid to the process than about any major disagreements, although some definitions were amended, and smaller issues added. After that, the proposal followed the typical flowchart with parliamentarian readings, voting, more readings, more voting. This procedure was combined in a consensus draft report, and the European Parliament subsequently came up with a version with agreed and proposed changes (European Parliament, 2021a). Lastly, and all formally organised according to the standard regulation, trilateral negotiations between the European Commission, the member states representatives in the Council of the subject area (Justice and Home Affairs Council), and the European Parliament took place. They culminated at the end of June 2022 in a consensus solution about the directive text (Council of the European Union, 2022a). Finally, a new CER Directive emerged, having a binding legal status on 27 member states (Council of the European Union (2022b).

This article asks what is at stake in this process of moving from one directive to another. Why has the concept of protection been replaced by the concept of resilience, and why has the concept of critical infrastructure been replaced by the newly invented euro-concept of critical entities? What are these entities and which sectors of CI do they represent? What is the risk picture behind the new directive; who or what is threatening European infrastructure? Are the prioritised risks physical or cyber, or both, and how are they interrelated? How does the new directive deal with the fact that while the member states are formally responsible for safeguarding their critical infrastructure, most of them are owned, administered and operated by private, and often foreign or multinational companies? Perhaps most importantly, in the penultimate section we discuss the European integration dimension of this new directive; what does it tell us about the current dynamics of European integration, and how it could be explained?

In the conclusions, we highlight several challenges in the current CER Directive that should be understood and properly approached early on. This is particularly important when the 27 member states start to implement the rather far-reaching and complex directive in

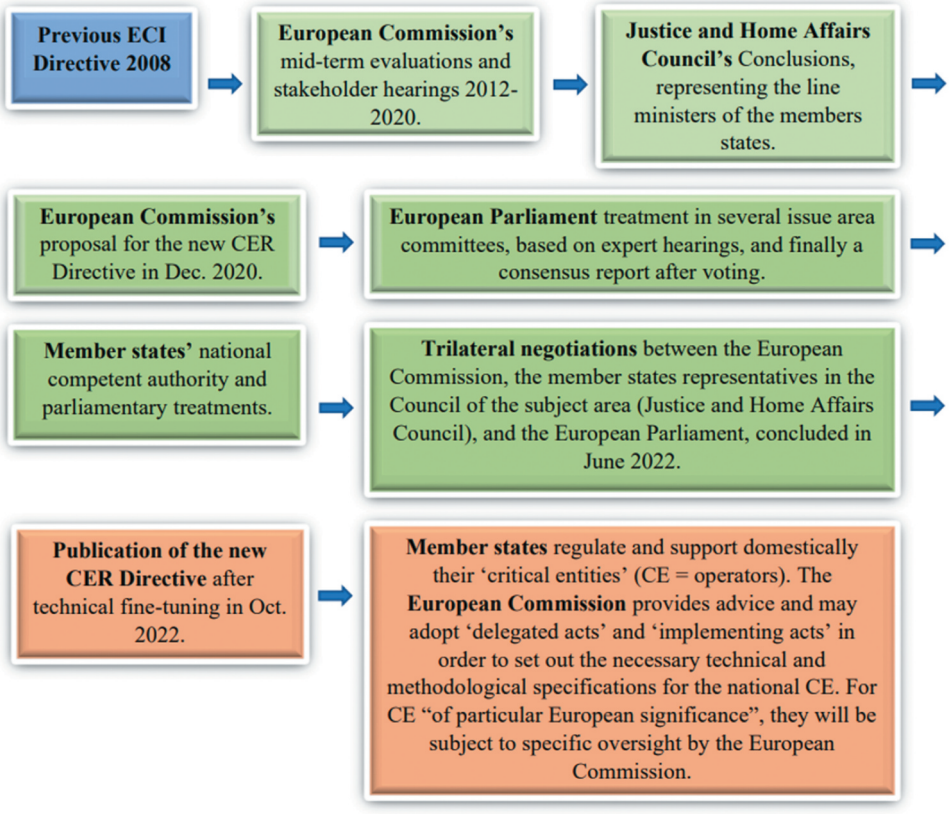


**Figure 1.** The policy process towards the CER directive.

the context of a variety of languages and administrative cultures – in order to avoid confusion and unintended consequences.

## 1. Methodological note and theoretical underpinnings

We will combine a typical public policy document study with a consideration of the relevant scholarly research on CI and its resilience. Being a desk case study and focusing on EU CI policy development, the methodological approach is a structured comparison between the previous ECI Directive (2008) and the new CER Directive (2022), together with lower-level policy documents. This comparative approach aims at identifying their central differences and similarities as well as the main development tendencies.

The more scholarly CI research literature is then utilised to problematise and deconstruct the underlying assumptions embedded in the described developments. While the article does not aim at developing any new theory, it summarises the main academic debates in the central areas that the CER Directive deals with. The assumption is that the EU policies have been considerably affected by this academic research, while at the same time those policies open up or prioritise new research avenues.

As mentioned above, the potentially more profound theoretical and political question is why the EU member states would voluntarily let the EU become more powerful in regulative terms in a field that belongs to their mandate and sovereignty. This kind of question is a more generic political science issue, also applicable to other domains of European public policy studies beyond the current CI domain. To this effect, at the end of the article, we identify three well-known integration theory schools, namely functionalism, the multi-lateral governance approach, and agent-principal theory, which can be applied to the current issue and facilitate at least some theoretically-grounded explanations.

## 2. Why resilience, and what does it mean?

The first issue to discuss is the paradigmatic change from protection to resilience in CI. Given that 'resilience' has practically become an all-encompassing part of scientific discourse and political jargon during the past decade, and a panacea of sorts for all problems, what does this change mean for the CI domain?

### 2.1. From protection to resilience

When the European Commission started to pay attention to CI, particularly by launching the European Programme for Critical Infrastructure Protection (EPCIP) in the mid-2000s (European Commission, 2006a; cf. the preparatory documents by the, 2005, 2004), the focus was clearly on CI protection (often abbreviated to CIP). The same goes for the ECI Directive proposal (European Commission, 2006b) and the later, finalised ECI Directive (Council of the European Union, 2008). While the EPCIP recognised that not all infrastructures can be protected against all threats, the solution was to prioritise the selected CI sectors and a set of threats against which they should be protected. Thus, the question was largely about traditional risk management in order to avoid and prevent unwanted events in certain CI sectors.

Indeed, the broader concept of resilience did not appear in the policy documents of that time at all (Pursiainen, 2009, p. 727). In the European Commission (2012) review of the EPCIP, resilience already played a role, albeit a small one. As an alternative concept to protection, resilience did not, however, start to appear in earnest in the European Commission in the context of CI until about 2014 (Pursiainen & Gattinesi, 2014). Meanwhile, the concept of CI resilience (sometimes abbreviated to CIR) had become a commonplace in more scholarly academic debates. In the EU Horizon 2020/current Horizon Europe research funding programmes, at least since 2014, the CI-related calls and respective approved projects have essentially not been about CIP but about CIR. As such, this leads to a broadening and deepening of the research scope.

Resilience, in general terms, refers to 'before, during and after' the unwanted event or disruption of the CI, thus covering the whole crisis management cycle (Pursiainen, 2017). In CI, this means that it includes pre-crisis protection – paying attention to such issues as robustness and the ability to withstand or resist stress – but also assumes that CI disruptions will sometimes inevitably take place and cannot be avoided. Therefore, one also has to enhance absorptive and adaptive capabilities, such as redundancy, as well as recovery strategies (e.g., Cantelmi et al., 2021; Gritzalis et al., 2019; Liu & Song, 2020; Mottahedi et al., 2021; Rehak et al., 2019; Rød et al., 2020).

In the 2020 CER Directive proposal, this issue is already duly noted, even being one of its main

justifications, namely, '*it is necessary to fundamentally switch the current approach from protecting specific assets towards reinforcing the resilience of the critical entities that operate them*' (European Commission, 2020a, p. 2, italics added). In this context, '"resilience" means the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity' (European Commission 202a, Article 2/2, p. 23). This actually pretty well follows the mainstream definition in the CI resilience literature. The paradigm change is presented as arising, on the one hand, from the increasing number of member states, which 'are more and more informed by resilience thinking, in which protection is but one element alongside risk prevention and mitigation, business continuity and recovery' (European Commission, 2020a, p. 1). More formally, the reference is to the Council Decision from 2019, which is essentially on hybrid threats but includes a section on CI in this particular malicious threat context; it encourages the European Commission to consult member states about a 'proposal for a revision of the [ECI] Directive early in the new legislative cycle, including potential additional measures to enhance the protection and resilience of critical infrastructure in the EU' (Council 2019, decision point 27). From this, the European Commission concluded in its proposal a year later that it is necessary to ensure 'a more common approach to the resilience of critical entities in a number of sectors across the [European] Union' (European Commission, 2020a, p. 5).

What then is this 'more common approach to resilience of the critical entities' in the CER Directive? From an academic point of view, the new proposal did not go very far. True, it distinguishes between 'operator-level and systemic resilience' (European Commission, 2020a, p. 5), but precisely the way in which this 'systemic resilience' should be defined is not quite clear. For the member states, however, the mere jump from protection to resilience itself is crucial as it forces them to rearrange national practices, regulations and structures. Similar developments also took place within NATO around the same period, thus consolidating this from-protection-to-resilience paradigm change practically throughout Western Europe.

### 2.2. How do we know that a CI is resilient?

The broadening of the scope with the introduction of the concept of resilience is subject to some challenges. One of the main ones relates to how one can know that a CI (or a CE) is resilient. What is the scientific basis for assessing, or perhaps even for measuring, CI resilience? How does this resilience assessment differ from traditional risk assessment?

*Risk* assessment (or analysis) and management as a whole is a well-researched and even standardised field (e.g., ISO, 2018; ISO/IEC, 2019). Furthermore, from 2013 onwards, EU member states have already been obliged to conduct national risk assessment based on EU Civil Protection Mechanism legislation also including the CI domain, largely relying on the ISO standards (Pursiainen & Rød, 2021). By contrast, there is no jointly established, broadly shared or standardised understanding of how to assess and manage CI *resilience*. This is actually the quintessential challenge of any CIR or CER policy and management. Namely, before one can enhance resilience, one has to know how resilient the CI/CE currently is – and in which areas it lags behind the required resilience level – in order to enhance resilience in the first place.

True, in the academic field, there is an increasing methodological body of literature on how to measure CI resilience (e.g., AIIC, 2016; ANL, 2013; Gasser et al., 2021; Hollnagel, 2017; Lee et al., 2013; Linkov et al., 2014; OECD, 2014; Panteli & Mancarella, 2017; Rehak et al., 2019; Rød et al., 2020; Sun et al., 2020). In the CI domain, three resilience domains are most relevant, namely societal, organisational and technological. Societal (or community) resilience focuses on the effects of CI disruption on the population and vital societal functions of the affected community. Organisational resilience is about the effect of crisis management on the organisational and inter-organisational levels, often dealing with issues such as preparedness, early warning, response capacity, communication, and so forth. Technological resilience is then more about the very facility, its robustness, adaptability, redundancy, restoration and recovery capacity. The famous 'resilience triangle' (popularised by Bruneau et al., 2003) is usually the baseline for these kinds of assessments, aiming at diminishing the triangle in all its dimensions, thus withstanding the stress longer, adapting swiftly, and recovering more quickly.

These resilience domains are obviously interlinked (combined with other resilience domains, e.g., economic or psychological). In a more methodological sense, two resilience assessment approaches stand out. Modelling, and the ensuing simulations, make it possible to test the resilience of CI with digital twins. It may reveal some bottlenecks or weak points in a system, and help in decision-making. A systematic indicator-based approach, instead, demands a well-designed list of indicators, sub-indicators, their respective weightings, and algorithms to calculate the aggregated resilience. Sometimes software 'dashboards' are developed to this

effect, to create a 'resilience index' that serves as a metric of sorts for the CI's resilience. This type of work is never-ending, and is basically the same as risk management, the difference being that one expects the unwanted event to have taken place. In both cases, typically, the multiple uncertainties and interdependencies remain a major challenge.

However, outside the academic world, ultimately the issue of CI resilience assessment or measurement remains underdeveloped – or, rather, understandardised. Now, in its proposal for the CER Directive, the European Commission throughout the document suggests that the CER should be achieved based on risk assessment. This approach has not been changed in the process of drafting the final directive. This is, in the longer term, not methodologically sound. In contrast to the pre-event character of risk assessment and management, besides prevention and mitigation, CI resilience also emphasises preparedness, response, and rapidity of recovery applied during and after the event. In other words, unlike in risk management, unwanted events and surprises are anticipated to occur, as prevention and mitigation are not always sufficient (Park et al., 2013).

The challenge here then is that if a European regulation demands CER or CIR from the member states, one should create a relatively shared understanding of what resilience means in this context; how it could be assessed and, on this basis, how it could be enhanced beyond mere traditional risk management. Otherwise, all the member states will conduct it in their own way, which would lead to different versions of implementation of the new directive, and essentially also affect the amount of relative resources that are allocated for CI resilience in the member states.

The more positive side of this problem is, however, that risk management, which is already largely adopted by the industry, can be seen as a part of broader resilience management. True, some scholars differentiate between risk and resilience as rather antagonistic schools of thought and advise keeping them separate in order to avoid ill-judged investments (Linkov et al., 2018). Yet others propose a unified risk-resilience approach (Aven, 2019; Rød et al., 2020). We hold the latter opinion. A reasonable approach is to map CIR management against the definitions and concepts already used for risk management, particularly those of the ISO 31000 family of international standards (ISO, 2018; ISO/IEC, 2019). This approach has an advantage in that as many CI organisations are already familiar with the standard, they use it in their daily work. Thus, aligning the resilience elements with existing widespread risk management practice, rather than proposing a completely new scheme, could be the solution (Rød et al., 2020). This requires both proactive (risk prevention and mitigation) and reactive (absorptive, adaptive and recovery) resilience approaches and capacities.

Indeed, during the process of confirming the CER Directive, the role of standardisation was raised but not resolved. Should one not be capable of jointly defining how to assess CI/CE resilience, the directive is doomed to fail. The paradigm shift from protection to genuine resilience is then unlikely to be operationalised but just may give a false feeling of resilient CI.

In preparing a European standardisation organisation CEN/CENELEC or more global ISO standard to this effect, one could rely on such maxims as: no duplicate practices; tailorability; measurability; relative ease of use; and plurality of assessment techniques (Rød et al., 2020). The latter notion of 'plurality' would follow the ISO 31000 risk management approach, which allows any developed assessment technique or methodology to be used, or their combinations, depending on the specific needs and resources, while the basic principles of the standard should be defined and followed (cf., ISO/IEC, 2019).

## 3. What is a critical entity?

As is the case with moving 'from protection to resilience', a further change in the European Commission proposal was to move from the concept of CI to 'critical entity', or CE. So, what is a critical entity compared to critical infrastructure? Does it merely reflect a vocabulary change, or does it entail something else? We hold that the change may appear to be merely a minor vocabulary amendment, but it also denotes a paradigmatic dilemma of sorts. We think that it entails a change from CI sectors to CI operators, thus narrowing down the level of analysis and action.

This is also related to another issue. Namely, the CER Directive is aimed at enhancing the resilience of 'critical entities', which are critical for 'the maintenance of vital societal functions or economic activities in the internal [single] market' (European Commission, 2020a, p. 4). Connecting CI to the internal market in the EU, which is the core of European integration, brings a new analysis level into the picture, broader than entities and sectors. An internal or single market means a customs union that has common policies on product regulation and freedom of movement for all the factors of production (goods, services, capital, and labour). Further, the above quotation also raises the question of what the aforementioned 'vital societal functions' refer to.

### 3.1. A critical entity is a critical infrastructure operator – or is it?

One point in the CER Directive (European Commission, 2020a, pp. 1.4.1, 38, italics added) made mention of '*operators (referred to here as "critical entities")*'. No proper justification for this new concept is provided. Probably, it aims at moving smoothly from CI sectors (such as energy) towards more concrete operators (such as an energy company) or perhaps a facility (a power plant) to enhance and facilitate more detailed monitoring and regulation.

However, it is still not clear why the widely used 'CI operator' concept is not utilised. The problem with the 'new euro-language' is obvious. Should one take a look at the different official translations of what a 'critical entity' means in various language versions of the CER Directive (the directives are translated into all official languages of the EU), we may note that in German, for instance, it becomes *Einrichtung*, approximating 'facility' in English; in Finnish *toimija*, which would be translated as an 'actor' or 'agent'; in Italian *soggetto*, meaning a kind of responsible subject; in Swedish it is directly translated as *entitet*, which in this language, however, essentially refers to some kind of whole; and so forth.

One may then ask whether the vocabulary is rationally chosen. Can it be so that it leads to diverse national interpretations and applications, particularly given the complicated private and public ownership structures of the national CI in a variety of combinations? The issue becomes more serious as the new directive is justified by the EU internal (or single) market, following common rules. There is a long-standing debate that the member states differ in their compliance with the EU directives, for various reasons, but typically reflecting the differences in their political-administrative cultures (e.g., Zhelyazkova et al., 2016). On the other hand, it has been argued that the EU has recently managed to develop new tools for enforcing compliance and implementation (e.g., Börzel & Buzogány, 2019). However, it seems that unclear concepts, open to multiple interpretations, may negatively affect compliance and thereby enhance the competitive position of those member states who define the CE more loosely.

### 3.2. Paying lip service to vital societal functions as a deductive approach?

Perhaps a more important issue is what are those 'vital societal functions' that are mentioned as critical for the internal (or single) market? As early as 2012 in the European Commission's (2012) tentative self-appraisal evaluation of the EPCIP, there was a notion 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'. This refers both to the 'systemic resilience' between the critical systems as well as the fact that one should not restrict this to mere facilities.

Indeed, the understanding of the vital/critical societal functions, being broader than mere infrastructure, has always been adopted in facto by several member states, especially in Northern Europe (cf., Pursiainen, 2018, pp. 633–634). To exemplify this approach, for instance, the Norwegian system (not part of the EU but part of the European Economic Area, or EEA, and thereby closely involved in the EU in all aspects) starts from the 'societal needs', which are covered by 'vital or critical societal functions'. The latter depend on 'infrastructures' whose criticality is assessed by 'dependability', 'alternatives' or redundancy, and 'tight coupling'. This assessment forms the basis for deciding whether a certain infrastructure is critical or non-critical (NOU, 2006). Such basic needs can, for instance, be 'governability and sovereignty', 'security of the population', and 'societal functionality'. These can in turn be divided into subcategories of vital societal functions, such as public administration, electricity, food security or emergency services, and so forth (DSB, 2017).

Now, it seems that the European Commission has decided to cover vital societal functions, critical infrastructure sectors, and critical infrastructure entities in the same package. The issue here is that the new directive's unit or level of analysis is a critical entity, namely an operator, and not the vital societal (and economic) functions. It thus takes an inductive, bottom-up or agent-based approach. We do not claim that these different levels are antagonistic. But we argue that this kind of legislative approach makes it difficult to distinguish the critical infrastructure from non-critical as there is no clear methodology regarding what an entity is, and in which conditions it is critical. Namely, by definition, a resilient system should have some redundancy and one should not be too reliant on any entity's or operator's criticality. From a societal perspective, this conceptual and paradigmatic choice, moving from individual CI facilities towards vital societal functions, would thus allow a more resilience-seeking approach than the CER Directive suggests.

## 4. Increasing the criticality of everything?

The challenge of the EU CI policies has from early on been about how to draw the line between the EU

competencies and those of the member states. It is worth recalling that this field basically still belongs to the latter's mandate, but now, when the CER Directive is connecting the European CER to the EU internal (single) market, it will by definition become more European in terms of the mandate. This in turn culminates in the issue of what constitutes a CI/CE, and which of the multiple CIs could be understood as European CI (or ECI), or such critical entities that fall under the new CER Directive.

### 4.1. How many critical sectors are critical for Europe?

The issue of which CI sectors should be regarded as European was discussed at some length when preparing the 2008 ECI Directive. It was even discussed whether an ECI could locate outside of Europe if it affects the EU. That discussion was then soon closed. The European Commission (2006b, Annex 1, p. 21) originally proposed eleven CI sectors altogether with twenty-nine CI sub-sectors. During the process of discussing the then submitted ECI Directive proposal in the European Parliament, more and more additional sectors were suggested. This seemingly disturbed some member states, who saw their sovereignty in the CI domain threatened. In the finally approved 2008 ECI Directive, therefore, *only two sectors*, energy and transport, were accepted as basically 'European', further detailed and divided into eight sub-sectors (Council of the European Union, 2008, L 345/75, and Appendix 1, p. L 345/81). This two-sector solution was even further limited to the infrastructure located in member states where disruption would have a significant impact on at least two other member states. Many meanings about how many affected member states should be needed were discussed, but two it became. In the ensuing years, information and communication technology (ICT) was often raised as a possible new CI sector to be added to the list of ECI as it was considered a horizontal CI sector.

Now, a considerable broadening of the European regulation in terms of CI sectors is covered in the CER Directive. Following the European Commission's proposal, it includes ten sectors, namely energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space (European Commission, 2020a, p. 3). In order to make the related directives more compatible, these sectors are purposively the same as in the simultaneously proposed cybersecurity NIS2 Directive (European Commission, 2020c).

### 4.2. Interdependencies and system of systems

The challenge lies in how to define the 'critical entities' within these 'critical infrastructure sectors'. The CER Directive is fundamentally based on the broader challenge of dependencies and interdependencies. These refer to at least three different types of interrelationships, namely those between different sectors, between countries, and between the physical-digital interfaces. However, this becomes even more complex when we actually discuss the 'systemic resilience' of the CER in the sense that it is described in the European Commission proposal; or the 'system of systems' as it is typically referred to in the CI literature. In principle, the whole supply chain of any critical infrastructure sector duly becomes critical, including not only other CI sectors or critical entities, but also seemingly non-critical sectors or entities. This then is related to the so-called 'known unknowns', namely 'entities' that we know exist, but do not know that they are critical before a crisis occurs.

As mentioned above, in the explanatory section of the European Commission (2020a, p. 5), but not in the directive text itself, a distinction is made between 'operator-level and systemic resilience'. While the former risks are easily comprehensible, what then are the 'systemic risks' in the CI context? The directive proposal, and the approved directive, do not elaborate on this, but we get a hint from the 2021–2022 EU Horizon Europe calls (administered by the European Commission) that were prepared to provide scientific support to implement the new EU policy (European Commission, 2021a, pp. 96–112). The focus appears to be on resilience to 'different expected and unexpected events, emerging risks, be they natural or man-made, unintentional, accidental or with malicious intent'. These risks are systemic because of their 'systemic dimension and complexity of attacks and disruptions by cyber or physical means', including interdependencies within several types of infrastructure and due to their having a cross-border effect.

The academic blueprint approach to understanding CI interdependencies was already presented early on in 2001 (Rinaldi et al., 2001). In terms of the practical management of interdependencies, the issue is that when critical systems are rafted together, the critical elements of each become critical elements of all because of the possibility that failure in one part of one system will be externalised to others. Thus, the system-of-systems dilemma is that CI operators ('entities') typically know and effectively control the risks of their own system, but not those of other systems on which they are

dependent. There is already a plethora of theorising, modelling and simulations in reliability and resilience engineering showing that unexpected interdependencies often take or may take place. Should one take this information into account, one can simulate the best restoration strategies for interdependent CIs (e.g., Eusgeld et al., 2011; Ouyang & Wang, 2015; Thacker et al., 2017).

However, there is not so much empirical evidence of real-life CI disruptions that would be due to dependencies or interdependencies between different CI entities or sectors. This raises the question of what we know about interdependencies; the answer is that we do not know a great deal. In terms of conceptualising interdependencies, however, useful typologies have been suggested. If operations depend on the material output(s) of other infrastructure through a functional and structural linkage between the inputs and outputs of two assets, they are considered *physical*. If operations depend on information and data transmitted through the information infrastructure via electronic or informational links, they are regarded as *cyber*. If operations depend on the local environment, where an event can trigger changes in the state of operations in multiple infrastructures, they are termed *geographical*. And if operations depend on the state of other infrastructure via connections other than physical, cyber, or geographical, they are seen as *logical*, as this kind of (inter)dependency is attributable to human decisions and actions and is not the result of physical or cyber processes (e.g., Petit et al., 2018).

But are CIs dependent or interdependent? Dependency is the relationship between two critical products or services in which one product or service is required for the generation of the other product or service. Interdependency is a mutual dependency. However, there is a lack of European cross-sector or cross-border CI disruption databases, and the respective academic research. Some research (Luiijf & Klaver, 2021; Luiijf et al., 2009) nevertheless shows that around a third of the reported mostly national incidents in Europe result from incidents in other services. The energy (especially electricity) and ICT sectors are the main cascading initiating sectors. Energy seems to be the only sector that initiates more cascades than it ends up receiving. Even in this case, an energy sector CI failure typically triggers (only) two other CI disruptions, most of which are 'first-stage cascade' events.

To learn more about and build resilience against harmful and critical dependencies and interdependencies, it looks like a proper European database on CI disruptions would be useful, showing the real-life interconnections and dynamics, also taking into account multi-hazard conditions.

### 4.3. Artificial intelligence can help but may also add to the complexity

Ostensibly, an artificial intelligence (AI) approach is developing within the respective research to not only model and simulate system-of-systems interrelationships, but also to analyse, predict and provide decision support for CI operators. AI is aimed at replacing or supplementing human judgment and actions. In many ways, AI will be beneficial, automating the operation of CI, and even detecting and responding to cyberattacks and similar unwanted events (e.g., Begli et al., 2019; Kumar & Choi, 2022). AI and other emerging technologies (digital twins, Internet of Things etc.) have been argued to be needed particularly in dealing with climate change-induced CI emergencies, which are hard to predict or manage merely with risk management and inspections (Argyroudis et al., 2022). It is emphasised that proper standardisation is necessary for this purpose.

Yet it is obvious that if AI is used to assess potential risks, identify real-time threats and provide decision-making options for CI, or even to make the decisions somewhat detached from human control, it opens up new avenues for malicious cyberattacks against the input and output data and algorithms of the AI governing CI (e.g., Laplante & Amaba, 2021; Khurana et al., 2019). On the other hand, AI can also itself be, and already has been, used to create sophisticated cyberattacks (e.g., Kaloudi & Li, 2020).

True, the EU bodies are well aware of, if not yet prepared for, this threat. A proper Artificial Intelligence Act, proposed by the European Commission (2021b), is going through the European Parliament and Council to introduce regulatory control to this field. The proposed AI Act provides a list of high-risk AI systems, which include: 'Management and operation of critical infrastructure: (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity' (European Commission, 2021c, Annex II, 2a). Several other less physical systems that could be understood as being a part of CI are also mentioned under other subheadings of high-risk AI systems, such as law enforcement, border control, and the justice system. These systems have their specific requirements (European Commission, 2021c, Chapter 2) concerning, for

instance, such issues as risk management, data governance, technical documentation, accuracy, robustness and cybersecurity.

However, as one can imagine, on the basis of the current experience of constantly evolving cyber threats, and the mere fact that CI has become thoroughly integrated, cyber-physical systems (so-called CPSs), hackers, terrorists, criminals, and especially malicious foreign states will inevitably emerge to take advantage of the harm that can be caused by targeting the AI systems of CI, as well as creating malicious AI technologies to target CI.

## 5. The evolving risk landscape

When preparing the 2008 ECI Directive, choosing between terrorism or an all-hazards approach was one of the main issues at stake (Pursiainen, 2009, pp. 730–732). This was due to the fact that in the US, and consequently also in NATO, the newly emerged interest in protecting CI was a direct consequence of the 9/11 attacks. The Madrid 2004 commuter train bombings and the London 2005 underground terrorist attacks definitely shifted the upcoming EPCIP focus on terrorism as well. This led to a biased understanding of the causes of CI disruptions. So, how is this situation framed by the CER Directive?

### 5.1. From terrorism as a priority to an all-hazards approach

The decision to delegate CI issues to the then Directorate-General (DG) Home in the European Commission, instead of the DG that is responsible for civil protection, partially reflects this emphasis on terrorism. At the same time, in member states the respective competent authority could well be the one dealing with normal civil protection issues. Some kind of compromise was seemingly reached in formulating the final 2008 ECI Directive; it refers to an earlier Justice and Home Affairs Council call from December 2005 for the European Commission to prepare the EPCIP under the approach whereby '*manmade, 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*' (Council of the European Union, 2008, L 345/75, italics added).

It seems that the implicit tension between terrorism and an all-hazards focus in the earlier approach has been, if not completely resolved, at least better understood and the approaches better aligned. This is partly because the concept of hybrid threats was entering the picture, which, at the same time, served to further complicate the risk landscape. In the new CER Directive, the all-hazards approach has now been literally adopted, although it has been justified by the change of 'environment in which critical entities operate', and by the fact that 'the risk landscape is more complex than in 2008' (European Commission, 2020a, p. 2). Thus, it includes natural hazards, state-sponsored hybrid actions, terrorism, insider threats, pandemics, and major accidents, coupled with the challenges that new technologies such as 5 G or unmanned vehicles pose in terms of vulnerabilities. The theme of sectoral interdependencies and cascading effects is also forcefully conveyed.

A highly related issue, and a kind of variable, is whether European policies should be focusing on mainly physical threats or whether they should pay attention to cyber threats as well. In the early European (and also US) policy, cyber threats were typically discussed as a separate CII, that is, critical information infrastructure protection, not really part of CI policy (Pursiainen, 2009, pp. 728–730). The solution was initially to focus on both, but in practice the integration of both physical and cybersecurity threats was only in its infancy when preparing the ECI Directive in 2008 and these two fields of CI protection remained rather siloed.

The CER proposal and subsequently Directive seem to be well coordinated at a general level with the cybersecurity directives (NIS, NIS2). In 2016, it was proposed that the then still rather new NIS (Council of the European Union, 2016) would be replaced just four years later by NIS2 (European Commission, 2020b). This was largely justified by the rapid digitalisation of the internal (single) market and other activities due to Covid-19. The NIS2 proposal was published on the same day as the new CER Directive proposal, seemingly forming an interrelated package of European legislation.

However, the more complicated the threat picture becomes, the more difficult it is to define proper resilience strategies for CI. Besides accounting for independent hazards, one also has to develop withstanding, absorptive, adaptive and recovery models and strategies for a more complex, multi-hazard context, with cyberattacks, natural disasters, pandemics and human-induced hazards potentially taking place simultaneously in different combinations and dynamics (Argyroudis et al., 2020). As all the hazards or their combinations cannot be forecast, prepared for, or even simulated, scholars of crisis management have been quick to point out that it is difficult to produce a single preparedness plan that covers all the potential challenges emerging from crisis situations. Thus, contingency planning should actually be more about planning how to

improvise. Hence, both proactive (in advance) and reactive (when the crisis hits) resilience strategies should be available. In any case, planning should not be too rigid and should not pose an obstacle to improvisation (McConnell & Drennan, 2006; Stern, 2013).

### 5.2. Hybrid risks further complicating the issue

While phenomena such as climate change and new technologies sometimes result in unexpected or emerging risks, a specific risk category, namely malicious hybrid threats, is also emphasised in the CER Directive. However, it does not elaborate on these threats. In the earlier policy documents to this effect (Council of the European Union, 2019), hybrid threats typically include, for instance, cyberattacks, malicious foreign direct investments, disinformation, and automated vehicles – which could all be tools of malevolent actions against European infrastructure. The 2020 edition of the *Overview of natural and man-made disaster risks the European Union may face* (European Commission, 2021d, e.g., p. 130) provides a slightly more detailed picture of a malicious hybrid strategy that might combine physical attacks and cyberattacks with disinformation campaigns, changing ownership structures or deploying foreign-sourced components.

This gives rise to the problem that many of the above-mentioned elements of hybrid threats – *hybrid* in the sense that they would be applied simultaneously or in cascading mode in a variety of combinations – are beyond the reach of any one 'critical entity'. It would namely presuppose some kind of well-coordinated cross-sectoral and multinational operative cooperation, perhaps combined with AI. The practical issue then is how a member state, committed to liberal values, coordinates the defence against hybrid threats involving CI, without infringing the main principles of this market-based liberalism by establishing some multi-sectoral operative body or 'critical entity' to manage the crises. This naturally leads to the discussion of public-private partnership or other multi-level governance models.

## 6. Public-private partnership or more regulation?

While governments are understood as being responsible for safeguarding the CI in the EU context, most of this CI is increasingly owned, administered and operated by the private sector. Governments simply lack the monopolised authority, knowledge and resources to actually fulfil the responsibility of securing the resilience of their CI. This is further complicated by the sometimes multinational or foreign ownership structures of CI sectors. What therefore would the situation be like after the new CER Directive?

### 6.1. The member states regulate

The issue was implicitly a challenge for European CI policy from early on. Basically, the alternatives consist of adding regulation, or CI companies' self-regulation to avoid state regulation, or some kind of combination in terms of an idealised public-private partnership (PPP). As profit-seeking companies within a largely competitive business environment, it is unlikely that the CI sectors, operators or entities would self-regulate any more than was strictly necessary.

The logic of the CER Directive is that it regulates the member states, and the member states are obliged to regulate their CE/CI. But what does this regulation entail in terms of PPP? The CER Directive seems to signify a step towards more regulation, albeit mostly delegated to the member states. This is most notably presented in the CER Directive Articles 9–19, thus covering more than a third of the directive's 26 Articles. This marks a considerable increase in attention paid to regulation, although the message is not quite clear-cut. Regulation is formulated in the spirit that regulation by the state is actually a 'support' for the private or public companies that operate CI. A member-state government is expected to provide such support for critical entities in the form of material, methodologies, and training in order to ensure their resilience.

It seems somewhat questionable, however, as to whether the governments have such capacities and capabilities, unless they start to considerably enhance their national CI research and thus work through the academic and research community. Voluntary information-sharing is also expected to take place between the competent government authorities and the CE. It is likely that this will as such become nothing more than a continuation of the previous PPP, should it ever have worked effectively.

However, the CER Directive also demands that the member state will identify the concrete CE objects, subject to the CER Directive, for each CI sector and subsector. This might be a tough task, and doomed to arbitrariness without any clear-cut criteria. However, a list of these CE objects should be provided to the European Commission and each such CE will be notified of their identification as a CE, with their respective obligations to regularly assess their risks on the basis of national risk assessments and then, in a well-

documented manner, to 'take appropriate and proportionate technical and organisational measures to ensure their resilience'.

This is clearly then a state-regulated burden for the CE, but also for government authorities as they have to streamline this kind of national CE regulation. Even more of a challenge is how to streamline the member states' approaches.

### 6.2. Or the European commission regulates?

What then is the European Commission's role in this process after the directive has been approved? There are some indications that the national CE are subject to external evaluation not only by the member states. By the invitation of the member states, advisory missions organised by the European Commission are to provide advice to CEs in meeting their obligations. The European Commission is further empowered to adopt 'delegated acts' and 'implementing acts' in order to set out the necessary technical and methodological specifications for the national CE. When it comes to CE 'of particular European significance', they will be subject to specific oversight by the European Commission. As it is not clear what this new regulatory practice would look like and in which cases it would be applied, the first practical experiences of this new practice remain to be seen.

In practice then, how might the European Commission have sufficient knowledge to support and advise member states in these kinds of rather complicated and often technological questions? Indeed, it may well have such expertise. One should recall, for example, the considerable promotion of research, development and innovation (RDI) by the EU, particularly Horizon Europe, a multi-hundred-billion programme, which has regular large-scale calls related to CI (European Commission, 2021a). In concrete terms, the projects alone, or in concert, produce practical guidelines, often tested in real CI and reaching a high Technology Readiness Level (TRL), as tested in practice. While the participants in the projects are individual research institutions, CI operators, and competent authorities, the European Commission is largely the agenda-setter and facilitator of EU policy-relevant research and policy advice. Another platform worth mentioning is the European Commission's own science and knowledge service, the Joint Research Centre (JRC), hosting thousands of researchers in several countries in almost all conceivable fields. In the field of CI, it includes, for instance, the European Reference Network for Critical Infrastructure Protection (ERNCIP, n.d.). The work of ERNCIP is organised in Thematic Groups (e.g., aviation, industrial automated control systems), bringing together hundreds of participants drawn from member-state experts working in industry, academia or competent authorities.

## 7. Creeping integration or a rational division of labour?

The discussion above inevitably leads us to ponder the whole issue in the much wider context of European integration and its dynamics. What would explain the fact that the member states have seemingly voluntarily, and during the past fifteen years increasingly, limited their sovereignty in a field that is not in principle supranational?

### 7.1. Not a tailored job but off the peg?

One should note that the European Union's increasing role within the field of CI policies and regulation is not an untypical development. It takes place in other fields as well, where the European Commission does not have clear-cut supranational power. This can be understood as a tendency towards what has been labelled 'creeping competence' or 'informal governance'. Such fields following the same line include, inter alia, the environment, regional development, research and technological development, energy, civil security, Common Foreign and Security Policy, and health policy (e.g., Pursiainen & Rød, 2021; Bergmann, 2019; Greer & Löblová, 2017; Riddervold, 2016; Riddervold & Rosén, 2016; Princen, 2016; Kirchner et al., 2015; Maltby, 2013; Princen & Rhinard, 2006; Christiansen et al., 2004; Pollack, 1994, 2000).

Yet the CER Directive has nonetheless been prepared in a duly democratic and transparent manner. The current solution was chosen as the national competent authorities and even CI operators representing different sectors seemed to support or even propose it in the preceding evaluation process (European Commission, 2019). The final directive is naturally also enforced by the member states and the European Parliament in a due and detailed process. All of these processes and respective bodies voluntarily transfer some regulatory, agenda-setting and decision-making power from national to supranational level, meaning the European Commission in practice. So what explains that?

### 7.2. A rationalist integration?

This development seems to support (at least) three somewhat interrelated 'theoretical schools', typically exemplified in European integration studies. In terms

of the traditional 'functionalist' approach (Haas, 1958), or its revised 'neofunctionalist' version (Haas, 1964, 1990; Schmitter, 2005), states voluntarily assign some expert-level duties, control, and authority to a supranational power in the name of their functionalist needs; things have to be done. In our case, this may well represent the logic of the national competent authorities who, in the course of fifteen years of dealing with this issue in the context of the previous ECI Directive from 2008, had come to the conclusion that a more centralised, efficient and broader EU regulation was needed to protect the national CI. While the Council (representing member states) and the European Parliament (representing nationally selected party politicians) probably rely on not only their ideology but also on expert views and lobbyists to a considerable degree, their positive approach can perhaps be additionally understood in terms of the growing superpower tensions from outside. This refers in particular to hybrid threats from Russia and China. The member states understand that their CI resilience is better handled within the EU, as opposed to them acting in isolation.

The aforementioned functionalist explanation includes some presuppositions about the converging belief systems of the relevant actors. But it is basically rationalist. Introducing the internal (or single) market efficiency argument in this context to justify more European regulation does not seem to be a mere pretext. Rather, it is a real consequence of increasing the interconnectedness of the European countries, or of the effort to defend this interconnectedness against external, malicious hybrid and cyber threats, in addition to such issues as unpredictable climate change-induced hazards, which are becoming more frequent and severe.

In more contemporary theoretical terms, the current case could also be regarded as an example of European 'multilevel governance' (Tömmel & Verdun, 2009), or a hybrid governance system, where nearly all policy areas are covered by the EU sooner or later. This happens either through formal competences or, as in our case, through rather smooth coordination and facilitation. Our case could then be explained by the claim that the structure of governance is supposed to reflect the efficient production of the public good (European CI resilience) and/or that governance should at least mirror the patterns of the community (the EU) where it takes place (Schakel et al., 2015).

Furthermore, the above-described development reflects the logic of the famous 'principal-agent theory' (De la Porte, 2011; Pollack, 2003). The governments (principal) delegate their power to the European Commission (agent) due to an asymmetry of information and resources, with the latter being able to obtain a better overview of European-level CI risks and how to manage them in a coordinated manner.

Common to all of the above theoretical schools is that they would explain the development of the EU policies on CI by emphasising the logical integration of policies within like-minded countries, basically sharing the same interests, in the context of facing more and more internal and external challenges related to interconnectedness, dependencies and interdependencies.

## 8. Conclusions: the challenges of implementation

Let us conclude by outlining a few challenges based on the above analysis, particularly those that are related to implementation of the rather complicated CER Directive in 27 countries with different languages and political-administrative cultures in the multilevel governance context of the EU's member states.

*Challenge 1*. This article has discussed the paradigmatic change of European CI policies from protection to the broader concept of resilience. The very process recognised to some extent the failure of the protection approach. Therefore, more attention should be paid to adaptiveness and recovery with regard to CI disruption. However, this also begged the question of how we can know whether a particular CI facility or respective CI sector is resilient. The issue is that without any jointly agreed-upon, or standardised, ways to evaluate or measure it, all the member states will develop their own solutions. Thus, we propose the standardisation of a certain basic level of assessing CI resilience.

*Challenge 2*. Our slightly critical attention was drawn to the introduction of the new term 'critical entity' to the current theme. This is explained by the European Commission as being equivalent to a CI operator. This as such means that the CE concept does not bring much innovation to the field. Rather, it confuses the regulative vocabulary with its various national translations. On the other hand, it seems to indicate a shift of attention away from CI sectors to the level of concrete CI facilities, operators or entities, without clearly articulating this as such. In so doing, it only pays lip service to the approaches that focus more on vital societal functions. The directive emphasises the 'entities', rather than building any holistic system with regard to how to secure the societies' basic needs.

*Challenge 3*. We also noted that the new CER Directive will considerably broaden the number of CI sectors that will potentially be regarded as European, subject not only to national but also to increasing supranational monitoring and regulation. Furthermore, the directive also introduces a system-of-systems level of CIs, due to the dependencies

and interdependencies between facilities, sectors and countries. However, this notion alone does not provide any tools for understanding the concrete dependencies and interdependencies, and how to deal with them. This obviously provides a lot of room for speculative regulation.

*Challenge 4*. In the new CER Directive, the risk landscape has been broadened, most notably by treating physical and digital risks as more interconnected compared to the previous directive; it also brings the complexity of hybrid threats into the picture. We noted that it might be difficult for any one 'critical entity' to defend against such hybrid threats, within their normal mandates. Obviously, much more coordinated cross-sectoral networks between different authorities, CI operators and other stakeholders would be needed nationally and at the EU level.

*Challenge 5*. Further, the issue of the CER Directive's impact culminates in its increased regulatory power over not only the member states, but also the individual CI facilities or CE. While the direct power is mandated to the member states, it seems clear that the European Commission can take action, at least should it identify some CE of 'European significance' that falls below the acceptable level of resilience, even if there are no jointly agreed-upon criteria or standards.

*Challenge 6*. While the CER Directive approach and objectives can be defended, and we are all for it in principle, the coming years will witness some challenges with regard to the ability of this directive to work smoothly towards its ends. The main negative potential is that the directive's implementation in its various fields may develop in multiple directions depending on the particular member state's approaches. This would not support developing the internal (single) market on a fair basis, but would be beneficial for member states that interpret the directive as loosely (cheaply) as possible.

*Challenge 7*. The EU started to develop its CI policies in the early 2000s, largely borrowing concepts and approaches from the US, which had started developing its policies somewhat earlier. Over the years, it seems that the EU has become more self-reliant in defining and designing its approaches. This can be seen in the vocabulary, for instance. However, the adoption of the concept of CI resilience seems to be a rather shared perspective among the developed market economies. The same goes for such challenges as increasing complexity and interdependencies as well as 'new' threats and emerging technologies. It is therefore essential that there are, and will be, platforms, both policy and academic as well as related to standardisation issues, that maintain the international dialogue with like-minded countries.

In summary, we conclude that the new CER Directive attests to increasing regulation of the CI sector, both broadening and deepening the supranational tendencies in this field. This most likely also reflects the generic direction of European integration from a functional or expert perspective. Should the CER approach achieve most of its objectives, the European Union would be more integrated in its CI policies and respective threat pictures than before.

This would mean that the member states and European citizens would demand even more European-level coordinated solutions instead of member states' individual policies, particularly in times of crises.

## Disclosure statement

The Coalition for Disaster Resilient Infrastructure (CDRI) reviewed the anonymised abstract of the article, but had no role in the peer review process nor the final editorial decision.

## Funding

The Article Publishing Charge (APC) for this article is funded by the Coalition for Disaster Resilient Infrastructure (CDRI).

## Notes on contributors

*Christer Pursiainen* is Professor of Societal Safety and Security at the Department of Technology and Safety, Faculty of Science and Technology, Arctic University of Norway (UiT), in Tromsø, Norway, since 2014. He has defended his PhD in Political Science/International Relations at the University of Helsinki in 1999. Previously Pursiainen has worked in leading management and research positions in such institutions as the European Commission's Joint Research Centre, JRC, Institute for the Protection and Security of the Citizen (Italy, Ispra); Council of the Baltic Sea States, CBSS (Sweden, Stockholm); Nordregio, Nordic Centre for Spatial Development (Sweden, Stockholm); Russian-European Centre for Economic Policy, RECEP (Russian Federation, Moscow); Aleksanteri Institute - Finnish Centre for Russian and East European Studies at the University of Helsinki; and the Finnish Institute of International Affairs, UPI-FIIA (Finland, Helsinki). His publications consist of about one hundred and thirty scholarly publications on a variety of themes, including societal security, crisis management, critical infrastructure protection and resilience, foreign policy analysis, and regional cooperation and integration.

*Eero Kytömaa* works as Ministerial Adviser at the National Security Unit of the Finnish Ministry of the Interior. He has a worked extensively on countering hybrid threats and resilience policy planning in Finland and within the EU and NATO. In the past years, Kytömaa has represented Finland in the European Council negotiations on the Directive on the Resilience of critical entities. In 2016-2019 Mr. Kytömaa worked at NATO HQ Defence Policy and Planning

Division, Enablement and Resilience Section, in the position of Resilience Staff Officer (VNC). Among other duties Kytömaa coordinated the work of IRCSG planning group which addressed issues such as operational guidance for priority access, maturity resilience modelling and energy interdependencies. In addition, he contributed to work strands related to the Baltic Sea Region security. Before joining the public sector Mr. Kytömaa worked at the Crisis Management Initiative (CMI), which is founded by Nobel Peace laureate and former President of Finland Martti Ahtisaari. His publications consist of articles on national security, countering hybrid threats and resilience.

## ORCID

Christer Pursiainen http://orcid.org/0000-0001-5611-1701

## List of acronyms

| | |
|---|---|
| 5G | fifth-generation technology standard for broadband cellular networks |
| AI | artificial intelligence |
| CE | critical entity |
| CEN | European Committee for Standardization |
| CENELEC | European Committee for Electrotechnical Standardization |
| CER Directive | European Union Directive on the resilience of critical entities |
| CI | critical infrastructure |
| CII | critical information infrastructure |
| CIP | critical infrastructure protection |
| CIR | critical infrastructure resilience |
| DG | Directorate-General (of the European Commission, e.g., HOME or ECHO) |
| ECI Directive | European Union Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection |
| EEA | European Economic Area |
| EPCIP | European Programme for Critical Infrastructure Protection |
| ERNCIP | European Reference Network for Critical infrastructure Protection (European Commission) |
| EU | European Union |
| Horizon Europe | Former Horizon 2020. Horizon Europe is the EU's key funding programme for research and innovation with a budget of €95.5 billion 2021–2027, based on targeted calls and competition. |
| ICT | Information and Communication Technology |
| ISO | International Organization for Standardization |
| JHA | Justice and Home Affairs Council of the European Union |
| JRC | Joint Research Centre (European Commission) |
| NATO | North Atlantic Treaty Organization |
| NIS2 Directive | European Union Network and Information Security Directive 2 |
| PPP | public-private partnership |
| RDI | research, development and innovation |
| TRL | technology readiness level |

## References

AIIC. (2016). *Guidelines for critical infrastructures resilience evaluation*. Italian Association of Critical Infrastructures Experts.

ANL. (2013). *Resilience measurement index: An indicator of critical infrastructure resilience*. Argonne National Laboratory.

Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, J., Gkoumas, K., Vousdoukas, M., Hynes, W., Carluccio, S., Keou, O., Frangopol, D. M., & Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management*, *35*, 100387. https://doi.org/10.1016/j.crm.2021.100387

Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. *Science of the Total Environment*, *714*, 136854. https://doi.org/10.1016/j.scitotenv.2020.136854

Aven, T. (2019). The call for a shift from risk to resilience: What does it mean? *Risk Analysis*, *39*(6), 1223–1224. https://doi.org/10.1111/risa.13270

Begli, M., Derakhshan, F., & Karimipour, H. (2019). A layered intrusion detection system for critical infrastructure using machine learning. In *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE) proceedings*, pp. 120–124.

Bergmann, J. (2019). Neofunctionalism and EU external policy integration: The case of capacity building in support of security and development (CBSD). *Journal of European Public Policy*, *26*(9), 1253–1272. https://doi.org/10.1080/13501763.2018.1526204

Börzel, T. A., & Buzogány, A. (2019). Compliance with EU environmental law. The iceberg is melting. *Environmental Politics*, *28*(2), 315–341. https://doi.org/10.1080/09644016.2019.1549772

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, T. D., Shinozuka, M., Tierney, K., Wallace, W. A., & Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, *19*(4), 733–752. https://doi.org/10.1193/1.1623497

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, *41*(3), 341–376. https://doi.org/10.1007/s10669-020-09795-8

Christiansen, T., Føllesdal, A., & Piattoni, S. (2004). *Informal governance in the European Union: An introduction*. Edward Elgar.

Council of the European Union. (2008). Council directive 2008/114/EC of 8 December 2008 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*. 23.12.2008, L 345/75-L 345/82.

Council of the European Union. (2016). 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*. 19.7.2016, pp. L 194/1-30.

Council of the European Union (2019). *Council conclusions of 10 December 2019 on complementary efforts to enhance resilience and counter hybrid threats*.14972/19.

Council of the European Union. (2022a) . *EU resilience: Council presidency and European parliament reach political agreement to strengthen the resilience of critical entities*. Press Release 608/22 28/06/2022.

Council of the European Union. (2022b). Council Directive "on the resilience of critical entities". *Official Journal of the European Union*. forthcoming in 2022.

De la Porte, C. (2011). Principal–agent theory and the open method of Co-ordination: The case of the European employment strategy. *Journal of European Public Policy*, *18*(4), 485–503. https://doi.org/10.1080/13501763.2011.560071

DSB. (2017). *Vital functions in society. what functional capabilities must society maintain at all times?*

ERNCIP. (n.d.). European reference network for critical infrastructure protection. https://erncip-project.jrc.ec.europa.eu/

European Commission. (2004). *Critical Infrastructure protection in the fight against terrorism*. Communication from the Commission to the Council and the European Parliament. COM(2004) 724 final. Brussels, 20 October.

European Commission. (2005, November 17). *Green paper on a European programme for critical infrastructure protection*. Commission of the European Communities. Com(2005) 576 final.

European Commission (2006a). *European Programme for critical infrastructure protection*. Communication from the Commission of 12 December. COM(2006) 786 final. Official Journal C 126 of 7.6.2007.

European Commission (2006b). *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*. Commission of the European Communities. COM(2006) 787 final. Brussels, 12 December.

European Commission (2012). *Commission staff working document on the review of the European programme for critical infrastructure protection (EPCIP)*. SWD(2012) 190 final. Brussels, 22 June.

European Commission (2019). *Commission staff working document. Executive summary of the evaluation of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. SWD(2019) 310 final. Brussels, 23.7.2019.

European Commission (2020a). *Proposal for a directive of the European parliament and of the Council on the resilience of critical entities*. COM(2020) 829 final. 2020/0365 (COD). Brussels, 16 December.

European Commission (2020b). *Proposal for a directive of the European parliament and of the council on measures for a high common level of cybersecurity across the union, repealing directive (EU) 2016/114*. COM(2020) 823 final 2020/0359 (COD). Brussels, 16 December.

European Commission (2020c). *Annexes 1 to 3. Annexes to the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the union, repealing directive 2016/1148*. COM (2020) 823 final. Brussels, 16 December.

European Commission (2021a). *Horizon Europe. Work Programme 2021-2022. 6. Civil Security for Society*. European Commission Decision C(2021)4200 of 15 June.

European Commission (2021b). *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts*. COM (2021) 206 final 2021/0106 (COD). Brussels, 21.4.2021.

European Commission (2021c). *Annexes 1-9. Annexes to the Proposal for a regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts*. COM(2021) 206 final 2021/0106 (COD). Brussels, 21.4.2021.

European Commission (2021d). *Overview of natural and man-made disaster risks the European Union may face: 2020 edition*. Directorate-General for European Civil Protection and humanitarian Aid Operations (ECHO). Publications Office.

European Parliament (2021a). *Report on the proposal for a directive of the European parliament and of the council on the resilience of critical entities*. Plenary sitting. 15. 10.2021. A9-0289/2021. (COM(2020)0829 – C9-0421/2020 – 2020/0365(COD)). https://www.europarl.europa.eu/doceo/document/A-9-2021-0289_EN.html

Eusgeld, I., Cen, N., & Dietz, S. (2011). 'System-of-systems' approach for interdependent critical infrastructures. *Reliable Engineering System Safety*, *96*(6), 679–686. https://doi.org/10.1016/j.ress.2010.12.010

Gasser, P., Lustenberger, P., Cinelli, M., Kim, W., Spada, M., Burgherr, P., Hirschberg, S., Stojadinovic, B., & Sun, T. Y. (2021). A review on resilience assessment of energy systems. *Sustainable and Resilient Infrastructure*, *6*(5), 273–299. https://doi.org/10.1080/23789689.2019.1610600

Greer, S. L., & Löblová, O. (2017). European integration in the era of permissive dissensus: Neofunctionalism and agenda-setting in European health technology assessment and communicable disease control. *Comparative European Politics*, *15*(3), 394–413. https://doi.org/10.1057/cep.2016.6

Gritzalis, D., Theocharidou, M., & Stergiopoulos, G. (Eds.). (2019). *Critical infrastructure security and resilience. Theories, methods, tools and technologies*. Springer.

Haas, E. B. (1958). *The uniting of Europe: political, social and economic forces: 1950–57*. MI UMI Books on Demand.

Haas, E. B. (1964). *Beyond the Nation-State: Functionalism and international organization*. Stanford University Press.

Haas, E. B. (1990). *When knowledge is Power: Three models of change in international organizations*. University of California Press.

Hollnagel, E. (2017). *FRAM: The functional resonance analysis method: Modelling complex socio-technical systems*. CRC Press.

ISO (2018). *Risk management—guidelines*. ISO 31000: 2018.

ISO/IEC. (2019). *Risk management—risk assessment techniques. Edition 2.0*. IEC 31010: 2019.

Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computer Survey*, *53*(1), Article 20. doi:10.1145/3372823.

Khurana, N., Mittal, S., Piplai, A., & Joshi, A. (2019). Preventing poisoning attacks on ai based threat intelligence systems. In *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP) proceedings*, pp. 1–6.

Kirchner, E. J., Fanoulis, E., & Dorussen, H. (2015). Civil security in the EU: national persistence versus eu ambitions? *European Security*, *24*(2), 287–303. https://doi.org/10.1080/09662839.2014.968133

Kumar, A., & Choi, B. J. (2022). Benchmarking machine learning based detection of cyber attacks for critical infrastructure. In *2022 International Conference on Information Networking (ICOIN) proceedings*, pp. 24–29.

Laplante, P., & Amaba, B. (2021). Artificial intelligence in critical infrastructure systems. *Computer*, *54*(10), 14–24. doi:10.1109/MC.2021/3055892.

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review*, *14*(1), 29–41. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000075

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M., & Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change*, *4*(6), 407–409. https://doi.org/10.1038/nclimate2227

Linkov, I., Trump, B. D., & Keisler, J. (2018). Risk and resilience must be independently managed. *Nature*, (Correspondence) 555 (7694).

Liu, W., & song, Z. (2020). Review of studies on the resilience of urban critical infrastructure networks. *Reliability Engineering & System Safety*, *193*, 106617. https://doi.org/10.1016/j.ress.2019.106617

Luiijf, E., & Klaver, M. (2021). Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set. *International Journal of Critical Infrastructure Protection*, *35*, 100471. https://doi.org/10.1016/j.ijcip.2021.100471

Luiijf, E., Nieuwenhuijs, A., Klaver, M., Van Eeten, M., & Cruz, E. (2009). Empirical Findings on Critical Infrastructure Dependencies in Europe. In R. Setola & S. Geretshuber (Eds.), *Critical Information Infrastructure Security. CRITIS 2008* (Vol. 5508, pp. 302-310. Springer). Lecture Notes in Computer Science.

Maltby, T. (2013). European Union energy policy integration: A case of European commission policy entrepreneurship and increasing Supranationalism. *Energy Policy*, *55*(100), 435–444. https://doi.org/10.1016/j.enpol.2012.12.031

McConnell, A., & Drennan, L. (2006). Mission impossible? Planning and preparing for crisis. *Journal of Contingencies and Crisis Management*, *14*(2), 59–70. https://doi.org/10.1111/j.1468-5973.2006.00482.x

Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies*, *14*(6), 1571. https://doi.org/10.3390/en14061571

NOU (2006). *Protection of critical infrastructures and critical societal functions in Norway*. Report NOU 2006: 6submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006. English Summary 1st of July 2006.

OECD. (2014). *Guidelines for resilience systems analysis*. Organization for Economic Co-operation and Development.

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety*, *141*, 74–82. https://doi.org/10.1016/j.ress.2015.03.011

Panteli, M., & Mancarella, P. (2017). Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Systems Journal*, *11*(3), 1733–1742. https://doi.org/10.1109/JSYST.2015.2389272

Park, J., Seager, T. P., Rao, P. S., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, *33*(3), 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Petit, F., Verner, D., Phillips, J., & Lewis, L. P. (2018). Critical infrastructure protection and resilience—integrating interdependencies. In A. Masys (Ed.), *Security by design. advanced sciences and technologies for security applications* (pp. 193–219). Springer.

Pollack, M. A. (1994). Creeping competence: The expanding agenda of the European community. *Journal of Public Policy*, *14*(2), 95–145. https://doi.org/10.1017/S0143814X00007418

Pollack, M. A. (2000). The end of creeping competence? Eu policy-making since maastricht. *Journal of Common Market Studies*, *38*(3), 519–538. https://doi.org/10.1111/1468-5965.00233

Pollack, M. A. (2003). *The engines of European integration*. Oxford University Press.

Princen, S. (2016). Agenda setting in the european union. From sui generis to mainstream. In N. Zahariad (Ed.), *Handbook of public policy agenda setting* (pp. 348–366). Edward Elgar.

Princen, S., & Rhinard, M. (2006). Crashing and creeping: agenda-setting dynamics in the European union. *Journal of European Public Policy*, *13*(7), 1119–1132. https://doi.org/10.1080/13501760600924233

Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection. *Journal of European Integration*, *31*(6), 721–739. https://doi.org/10.1080/07036330903199846

Pursiainen, C. (2017). *The Crisis Management Cycle*. Routledge.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*, 632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Pursiainen, C., & Gattinesi, P. (2014). *Towards Testing Critical Infrastructure Resilience*. Publications Office of the European Union.

Pursiainen, C., & Rød, B. (2021). National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*, *12*(2), 194–214. https://doi.org/10.1002/rhc3.12215

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection*, *25*, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

Riddervold, M. (2016). (Not) in the hands of the member states: How the European commission influences EU security and defence policies. *Journal of Common Market Studies*, *54*(2), 353–369. https://doi.org/10.1111/jcms.12288

Riddervold, M., & Rosén, G. (2016). Trick and treat: How the commission and the European parliament exert influence in EU foreign and security policies. *Journal of European Integration*, *38*(6), 687–702. https://doi.org/10.1080/07036337.2016.1178737

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25. doi:10.1109/37.969131.

Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, *36*(4), 04020039. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000795

Schakel, A. H., Hooghe, L., & Marks, G. (2015). Multilevel governance and the state. In S. Leibfried, E. Huber, M. Lange, J. D. Levy, F. Nullmeir, & J. D. Stephens (Eds.), *The oxford handbook of transformations of the state* (pp. 269–285). Oxford University Press.

Schmitter, P. C. (2005). Ernst B. haas and the legacy of neofunctionalism. *Journal of European Public Policy*, *12*(2), 255–272. https://doi.org/10.1080/13501760500043951

Stern, E. (2013). Preparing: The sixth task of crisis leadership. *Journal of Leadership Studies*, *7*(3), 51–56. https://doi.org/10.1002/jls.21298

Sun, W., Bocchini, P., & Davison, P. D. (2020). Resilience metrics and measurement methods for transportation infrastructure: The state of the art. *Sustainable and Resilient Infrastructure*, *5*(3), 168–199. https://doi.org/10.1080/23789689.2018.1448663

Thacker, S., Pant, R., & Hal, J. W. (2017). System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures. *Reliability Engineering & System Safety*, *167*, 30–41. https://doi.org/10.1016/j.ress.2017.04.023

Tömmel, I., & Verdun, A. (Eds.). (2009). *Innovative governance in the European Union: The politics of multilevel policymaking*. Lynne Rienner Publications.

Zhelyazkova, A., Kaya, C., & Schrama, R. (2016). Decoupling practical and legal compliance: Analysis of member states' implementation of EU policy. *European Journal of Political Research*, *55*(4), 827–846. https://doi.org/10.1111/1475-6765.12154