Accounting for systemic risk in analysis of crisis scenarios

Jose J. Gonzalez
Department of ICT, Faculty of Engineering and Science, Centre for Integrated Emergency Management (CIEM), University of Agder, Kristiansand, Norway
josejg@uia.no

Reem Abbas
Department of Computer Science and Software Engineering
Auckland University of Technology
Auckland, New Zealand
reem.abbas@aut.ac.nz

Sigurd Paulsen
Dept. of Organization, Crisis Management and Information Security,
Kristiansand municipality, Norway
sigurd.paulsen@kristiansand.kommune.no

ABSTRACT

Systemic risk is ubiquitous in our increasingly globalised world owing to the interconnections within and across sectors. However, a review of National Risk Assessments performed in OECD member countries reveals that systemic risk is rarely mentioned, and it is never accounted for in those assessments.

A powerful method accounts for systemic risk and identifies mitigating strategies using participatory modelling with stakeholders: strategy mapping with *Strategyfinder*. The risk model is represented as a directed graph consisting of risk nodes and directed edges (arrows) expressing causal influences. The method originated in the management of large, complex projects, and it has been applied to systemic risks in critical infrastructures and pandemics.

We demonstrate the *Strategyfinder* method using a scenario describing a cyberattack on electronic communication infrastructure leading to serious consequences for health and lives. The scenario is borrowed from the report Analysis of Risk Scenarios by the Norwegian Directorate for Civil Protection.

Keywords

National Risk Assessments, Risk scenarios, Disaster risk reduction, Vicious cycles, Cascading effects.

INTRODUCTION

A Wider Perspective of Systemic Risk

Systemic risk has been increasingly recognised during the last 2-3 decades as ubiquitous. While the disaster risk reduction community is aware of systemic risk in financial systems (Kim et al., 2022, p2; Schweizer, 2021, p90), the community is less conscious of the role of systemic risk in disruption and delays in complex projects (Gonzalez & Eden, 2023). Not being sufficiently aware of the literature on systemic risk in complex projects (e.g., Ackermann et al. 2007; Ackermann et al. 2011; Williams et al., 1997), the disaster risk reduction community has not yet adopted a validated approach of strategy mapping for disaster risk management using participatory modelling with a team of stakeholders (practitioners, and power-brokers). Using this approach, the team develops risk mitigations strategies deemed effective and practical. Recent evidence of the approach's applicability in disaster risk management has emerged (Abildsnes 2023; Bryson et al., 2023; Eden & Gonzalez, 2023).

Feedback Loops as Result of Interconnected risks

While there are many definitions of systemic risk, all mention feedback (a.k.a. circular causality) among its characteristics (Centeno et al, 2015; Flood et al., 2022; Gonzalez & Eden, 2023; Kaufmann & Scott, 2003; Kim et al, 2022; Reichstein et al., 2021; Renn et al., 2019; Schwarcz, 2008; Schweizer, 2021; UNDRR & UNU-EHS, 2022).

Systemic risk occurs because of the interconnections between risks. When risks give rise to further risks, as is the case in financial systems, in complex projects, and in many disasters, the consequences become very complicated. In all of them, a risk can cause a plethora of other risks, and significantly that risks reinforce themselves through feedback loops (a.k.a., vicious cycles).

Major disasters, like the COVID pandemic, trigger many vicious cycles across the critical infrastructures of nations (in fact, across the whole world). Cascading effects happen both within sectors and across sectors. The mitigation of systemic risks cannot proceed by mitigating separately single vicious cycles. Rather, the identification of the potency of risks – those risks with the most vicious cycles – is a must, to make those most potent risks the priority for risk mitigation measures (Gonzalez et al., 2021).

UNDRR Report on Systemic Risk Mitigation

Systemic risk has got prominent attention from the United Nations Office for Disaster Risk Reduction (UNDRR) in its two last reports on disaster risk reduction – counting together 730 pages. The Global Assessment Report on Disaster Risk Reduction 2019 (UNDRR, 2019), and the Global Assessment Report on Disaster Risk Reduction 2022 (UNDRR, 2022), are extensive reviews of the emergent science of systemic risk and of the challenges posed by systemic risk. In the following we refer to those reports as GAR2019 and GAR2022 for brevity.

GAR2019 states that systemic risks are triggered by the complexity and the interconnections of our increasingly globalised world, whereby the resulting networks determine the exposure and vulnerability shaping the dynamic interactions among the Sendai Framework, the 2030 Agenda, the Paris Agreement, New Urban Agenda, and the Agenda for Humanity (UNDRR, 2019, p32). Assessment and management methodologies for systemic risks are not yet part of the current operations of the twenty-first century risk management institutions; however, there is a growing sense of urgency for a paradigm shift (ibid, p44). The science of systemic risk and systemic risk management is still in "primordial state" (ibid, p146). GAR2022 asserts that little progress has happened in the three years since the previous global assessment report (UNDRR, 2022, p146).

However, the GAR2022 report fails to capture recent advancements utilising strategy mapping. Several publications (Abildsnes et al., 2023; Gonzalez et al., 2021; Gonzalez & Eden, 2022; Eden & Gonzalez, 2023; Gonzalez & Eden, 2023) and a recent report (Bryson et al., 2023, p24-30) describe the extension and application of the approach which emerged in complex project management to systemic risk in the COVID pandemic.

National Risk Assessments – A Fertile Ground for Systemic Risk Management?

The national civil protection agencies are tasked with maintaining a general overview of risk and vulnerability within society. Systemic risk became a hot topic for disaster risk reduction about 2-3 decades ago. Thus, it is natural to ask: do the national civil protection agencies account for systemic risk in their national risk assessments? If the answer is 'not yet', is there a fertile ground in future national risk assessments for using the recent advancements in strategy mapping (ibid)?

Our method to answer the question consists of two steps:

1. Check if a representative report on national risks assessments proves that systemic risk is being accounted for.
2. If the answer to #1 is 'no', apply strategy mapping to an existing national risk assessment to account for systemic risk.

We proceed to these steps in the following two sections.

IS SYSTEMIC RISK ACCOUNTED FOR IN NATIONAL RISK ASSESSMENTS?

For the first step, we examine the report on disaster risk analysis procedures by the Organisation for Economic Co-operation and Development (OECD). The OECD report presents a cross country perspective of national risk assessments including governance practices for National Risk Assessments and the assessment results in the 20 OECD countries including Australia, Austria, Canada, Denmark, Estonia, Finland, Germany, Hungary, Korea, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland,

United Kingdom, and the United States (OECD, 2018).

The OECD report states: "National Risk Assessments are used to support risk management decisions in a rapidly changing global risk landscape characterized by increasingly complex, interconnected societies and highly mobile people, information and goods." In increasingly complex and interconnected societies the risks become increasingly systemic.

Among the countries reviewed in the OECD report, New Zealand is the only country that included systemic risk in its key definitions, stating that systemic risks are those that "arise from the interactions between interdependent elements of the economy and society". One of the criteria used in New Zealand to characterise risks requiring a national response relates to have "multiple or inter-related problems which when taken together constitute a national or systemic risk".

However, none of the national risk assessments reviewed in (OECD, 2018) report systemic risks.

APPLYING STRATEGY MAPPING TO AN EXISTING NATIONAL RISK ASSESSMENT

For the second step, we examine if a 'promising' risk scenario implicitly accounts for systemic risk. By a 'promising' risk scenario we mean a very detailed scenario where risks cause cascading effects across several critical infrastructures.

The Norwegian Directorate for Civil Protection has been conducting national analyses of risk scenarios since 2011. The risk analyses take a social science approach and are based on qualitative data, expert assessments, and broad participation in the analysis processes. The analyses, which are updated regularly, are very detailed.

Among the 25 risk scenarios described by the Norwegian Directorate for Civil Protection in their last issue of Analysis of Crisis Scenarios (Norwegian Directorate for Civil Protection, 2020), we select a scenario which *a priori* could be expected to contain many interconnected risks, viz. scenario 18.2 "Cyber attack on electronic communications infrastructure" (Norwegian Directorate for Civil Protection, 2020, p204-207). The scenario describes a cyber attack against the central nodes in the transport network of the Norwegian telecommunications company Telenor. According to the national risk analysis, the attack would cause all electronic communication devices in Norway to fail completely for five days, with massive consequences on critical infrastructures, particularly on life and health.

In the scenario, Telenor's transport network for electronic communications is described as the only nationwide in Norway. The situation has changed since. But although two additional networks, Broadnet and Telia, increased its coverage since the report was produced, Telenor is still the largest transport network in Norway, with more than 200,000 kilometres of fibre and copper cables, and more than 10,000 base stations.

Therefore, the scenario 18.2 "Cyber attack on electronic communications infrastructure" described in the report by the Norwegian Directorate for Civil Protection (ibid, p204-207) is still suitable for answering the question whether the social science-based scenario analysis employed by the Norwegian Directorate for Civil Protection considers systemic risk.

Method

Reinforcing feedback loops of risks (a.k.a. vicious cycles) are the cause of escalating cascading effects. They must be expected in a massive cyber attack to the electronic communication infrastructure. Accordingly, we check whether the risk analysis of scenario 18.2 in (Norwegian Directorate for Civil Protection, 2020, p204-207) contains feedback loops. To be able to check whether the risk analysis of scenario 18.2 contains feedback loops we must first express the scenario as a formal model capable of being analysed for the existence of feedback loops.

Such formal model can be created with *Strategyfinder*™. *Strategyfinder* is a browser-based professional version of methods and tools developed at the University of Strathclyde since the 1990'ies. With *Strategyfinder* teams collaboratively work in person or virtually on messy problems, to develop strategies, and manage risks. However, in this paper we use *Strategyfinder* to create a formal risk model by reverse engineering scenario 18.2.

A *Strategyfinder* model of risks is a mathematical object known as a directed graph. In a directed graph there are nodes and directed edges ('arrows') expressing causality (i.e., that a node impacts causally on another node).

The nodes in a *Strategyfinder* risk model are risk statements: sentences of typically around 6-12 words describing risks. We adopt Lupton's (2013) definition of a risk: "a phenomenon that has the potential to deliver substantial harm, whether or not the probability of this harm eventuating is estimable".

The first step to create a *Strategyfinder* version of the scenario is parsing the description of scenario 18.2 to identify

the risks. Since *Strategyfinder* assigns a reference number to each statement, we number the risks in the order in which they are parsed in the subsections below.

The risks are listed in the subsections of the scenario 18.2 "Assessment of vulnerability", "Assessment of likelihood", "Assessment of consequences – Life and health", "Assessment of consequences – Economy", "Assessment of consequences – Social stability", and "Democratic values and capacity to govern". There is some redundancy in the scenario description: some risks are mentioned several times in different subsections. Hence, some statements which are obvious risks appear below without reference number (meaning that they are present in the *Strategyfinder* version using a slightly different wording).

In the following subsections we parse the text from scenario 18.2 (ibid, 204-207), labelling the risks with numbers in the same order as they appear in the scenario. In other words, we proceed by copy/pasting from scenario 18.2 and adding sequent numbers to each risk.

Parsed Risks from Scenario 18.2, Subsection "Assessment of Vulnerability"

[1] Telenor's transport network for electronic communications is the only nationwide one in Norway. [2] Broadnet has a transport network that covers 90 Norwegian towns and cities. However, [3] some of the infrastructure is shared with Telenor, and a [4] failure in Telenor's network would therefore also [5] knock out Broadnet's network. [6] Other electronic communications operators such as Telia, Ice, the emergency services' network (Nødnett) and others, mainly use Telenor's transmission infrastructure, and to some extent Broadnet's. [7] National radio and television companies rely on Telenor's transport network to get signals to transmitters. [8] Telenor's transport network is robust and well protected. However, in the event of [9] any network outage there are no alternatives. [10] Satellite telephony and radio communications do not have nearly enough capacity to meet the need for communication.

The most serious consequences are: [11] Management of the crisis at a political and administrative level becomes difficult, with [12] reduced opportunities for communication and coordination. The [13] disappearance of radio, television and the Internet means that [14] important information channels for the public would be unavailable. [15] Rescue efforts become more difficult in the [16] absence of telephony and when the [17] functionality of emergency numbers and the emergency services' network (Nødnett) is severely hampered. [18] Railway and air traffic would stop. [19] Road and maritime traffic would also experience problems. [20] Failures in payment services would cause [21] major challenges for the commercial sector and the public.

Parsed Risks from Scenario 18.2, Subsection "Assessment of Likelihood"

In this subsection of scenario 18.2 some of the statements are risk attributes, rather than risks themselves. We opt for considering them in the model, since the attributes have causal implications on the risks.

[22] Conducting a successful cyber attack as outlined in this scenario [23] requires a very high level of expertise and capacity – also with regard to intelligence. It is believed that only a [24] few actors have such capabilities. The likelihood would depend on the [25] international threat picture. The Norwegian Police Security Service's open threat assessment for 2018 states that "[26] enterprises within the Norwegian defence and public security sector, public administration, research and development and critical infrastructure are assessed to be particularly at risk of becoming intelligence targets." This applies with respect to [27] both network operations and more traditional intelligence gathering. [28] Several countries' intelligence services have interests within these areas.

Parsed Risks from Scenario 18.2, Subsection "Assessment of Consequences – Life and Health"

[29] Reduced opportunity to notify the emergency services in the event of acute events, [30] no possibility to call an ambulance in the normal manner, [31] inadequate communication and coordination between the emergency services, as well as [32] reduced efficiency and delayed treatment of patients in the health and care sector will have [33] consequences for life and health.

The analysis is based on an assumption that around 5% of acutely sick or injured people (who would otherwise have survived) would die. This means that, overall, the scenario would result in around 10 more deaths per day, or approximately 50 deaths in a five-day period, which represents [34] an increase of around 10% in relation to the normal daily mortality rate. [35] A number of planned treatments would be cancelled due to reduced efficiency. [36] During a five-day period, we estimate that 200–300 people would become significantly more ill due to reductions in the provision of treatment.

Parsed Risks from Scenario 18.2, Subsection "Assessment of Consequences – Economy"

It is assumed that the [37] direct economic losses will be NOK 2 to 10 billion and that they will mainly be associated with [38] the necessary repair and replacement of physical components and infrastructure.

The indirect economic losses will be associated with [39] loss of income, production losses and a decline in consumption, orders, and deliveries. A functioning payment system is a prerequisite for being able to pay for the delivery of goods and services, as well as the trading of financial instruments. Around a third of the normal production, or approximately NOK 13 billion, will be lost as a result of the loss of electronic communications. Even if some of the lost revenue can be recouped, it is assumed that [40] the net loss will exceed NOK 10 billion.

Parsed Risks from Scenario 18.2, Subsection "Assessment of Consequences – Social Stability"

The scenario would result in [41] significant reactions among the public in the form of anxiety, insecurity, fear and a feeling of powerlessness. The incident would be experienced as sudden and unfamiliar. A lack of information would significantly contribute to the level of anxiety. The reactions would be reinforced by [42] people involved in emergency situations being unable to get through on emergency numbers.

Parsed Risks from Scenario 18.2, Subsection "Democratic Values and Capacity to Govern"

The outage of electronic communications would cause [43] major challenges for governance and crisis management. The event would be perceived as a significant violation of shared cultural and democratic values, as well as basic individual rights and personal safety.

STRATEGYFINDER MODEL OF SCENARIO 18.2

The *Strategyfinder* model in this section sticks to the description of the risk scenario 18.2 provided in (Norwegian Directorate for Civil Protection, 2020, p204-207). Accordingly, from now on we will refer to the corresponding *Strategyfinder* model as the 'basic risk model'.

Fig. 2 on p7 displays the *Strategyfinder* basic risk model of the scenario 18.2. Explaining all the risk nodes and causal relations (represented by directed links, i.e., arrows) would be extensive. Hence, we use *pars pro toto* a restricted view produced with the *Strategyfinder* analysis tool 'dependency range' applied to #11 'management of the crisis at a political and administrative level becomes difficult' (Fig. 1 on p6). Fig. 1 shows only the risks and issues that directly or indirectly impact on #11.

First, notice that all the risks and issues shown in Fig. 1 are taken from the list of risks and issues parsed from scenario 18.2, cf. p4-5. Then, notice that some items, e.g., #9, #11, and #22, are formatted differently from the others. The reason for the different formatting will be explained below.

The arrow #12→#11 expresses that reduced opportunities for communication and coordination causes that the management of the crisis at a political and administrative level becomes difficult. The arrow #15→#12 expresses that absence of telephony causes reduced opportunities of communication and coordination. Hence, #15 impacts indirectly on #11. In addition to absence of telephony, the fact that in the event of an outage to the transport network there would be no alternatives means that #9 impacts directly causally on #11 in addition to doing it indirectly via #15. Thus, one has a direct causal impact on #11 expressed by the arrow #9→#11, and an indirect causal impact on #11 expressed by the series of arrows #9→#15→12→#11.

If there is an outage, risk #9 (no alternatives for electronic transport in case of an outage) causes #13, disappearance of radio, television, and the internet, hence the arrow #9→#13; crucial for that is the impact #7→#13, viz., that radio and television companies rely on Telenor's transport network to get signals to transmitters.

Multiple causes impact risk #9 ('no alternatives for electronic transport in case of an outage'):

- #4→#9, since failure in the Telenor's transport network directly impacts on #9, and because of #1→#9, that Telenor's transport network is the only nationwide one in Norway;
- #5→#9, since Broadnet, who could provide part of the electronic transport, is impacted #4→#5 from the failure in Telenor's transport network;
- #6→#9 expresses that other alternatives depend on Telenor or on Broadnet. Thus, no alternative operates in the case of the outage that knocks out Telenor and Broadnet.

The arrow #8→#4 is labelled with a red minus sign. Arrows with a red minus sign express *negative polarity*, viz., that *increasing* the cause *reduces* the causal impact. Here it means that the high robustness and degree of protection

of Telenor' network decreases the probability that a network failure happens. Arrows with positive polarity are in *Strategyfinder* not labelled with a + sign. I.e., no polarity sign means positive polarity by default.

Consider now #22 'conducting a successful cyber attack'. Risk #22 represents the desired outcome of the malicious agent. Hence, #22 has been formatted using the predefined *Strategyfinder* category 'STRATEGY'.

Conducting a successful cyber attack leads to failure of Telenor's network, hence the causal link #22 →#4.

Conducting a successful attack requires network operations and intelligence gathering by the malicious agent, expressed by #27→#22.

We skip explaining more arrows, since at this stage they should be self-explanatory.

The outcome #11 (the management of the crisis becomes difficult) is a goal for the agents behind the cyber attack. Hence, it has been formatted using the predefined *Strategyfinder* category 'GOAL'. Goals are outcomes desired on their own right. Goals have mostly only incoming arrows. Nevertheless, one can have goals (desired outcomes on their own right) one or two levels below a final goal. E.g., #12 ('reduced opportunities for communication and coordination in Norway') is arguably also a goal for the malicious agent. However, it is also a very busy node, with many ingoing and outgoing arrows, in the risk model. Hence #12 was rather formatted with the FOCUS category (red font), as were #9 and #32 for the same token (very busy nodes).

Strategyfinder has analysis tools to detect the busiest elements in the risk model (e.g., using the analysis submenu 'counting ingoing and outgoing links') and to detect 'heads' (elements with only ingoing arrows). The nodes #11, #34, #37, #40 and #41 are all 'heads' and have been formatted with the *Strategyfinder* category GOAL. Note that they are **negative** goals, i.e., intended outcomes of the cyber attack, which need mitigation strategies and actions on the side of the defenders (Eden, 2004; Eden & Gonzalez, 2023).

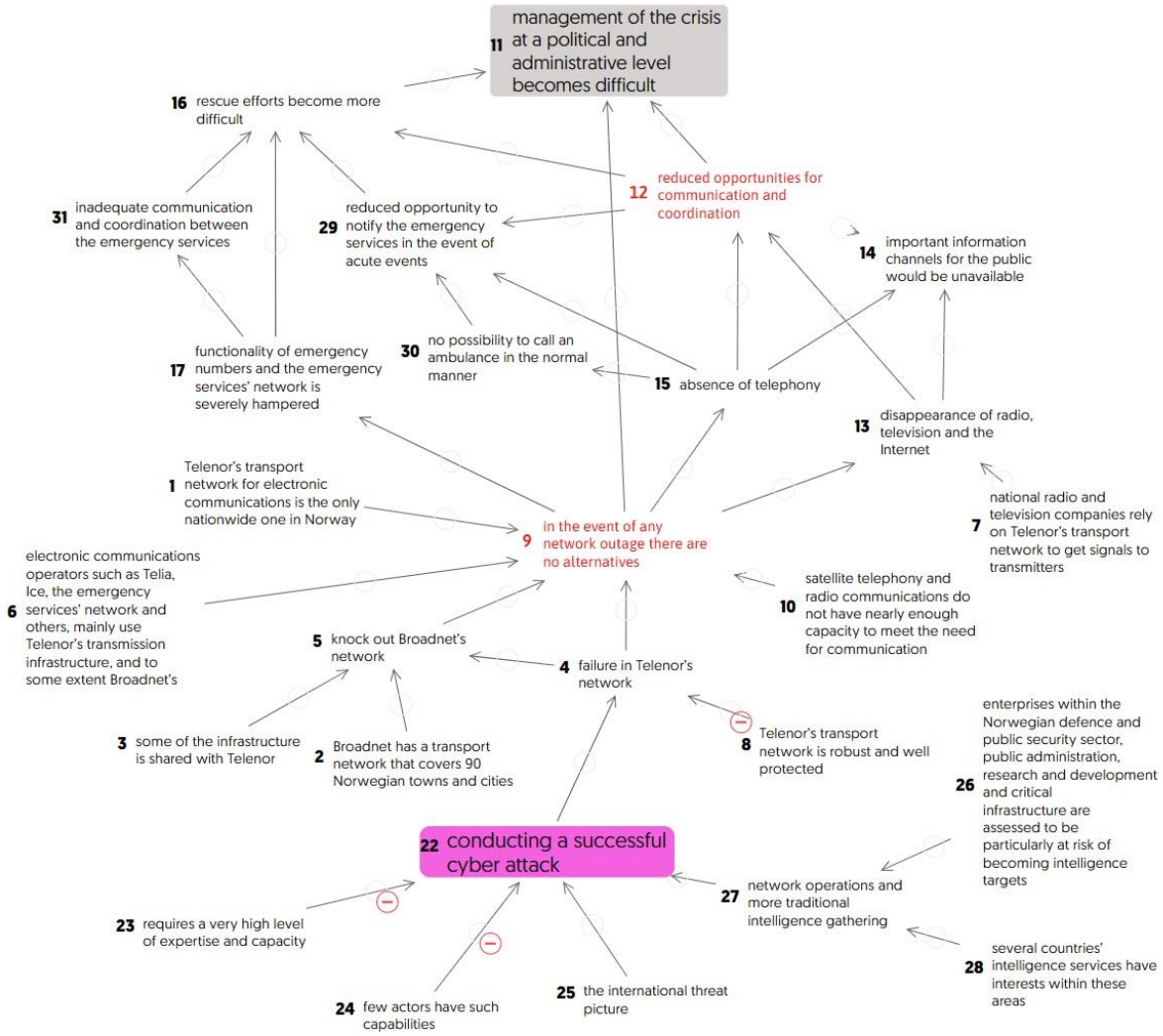

Figure 1 A restricted view of the basic risk model (shown in full on Figure 2) with the risks and issues that directly or indirectly impact on #11 'management of the crisis at a political and administrative level becomes difficult'.

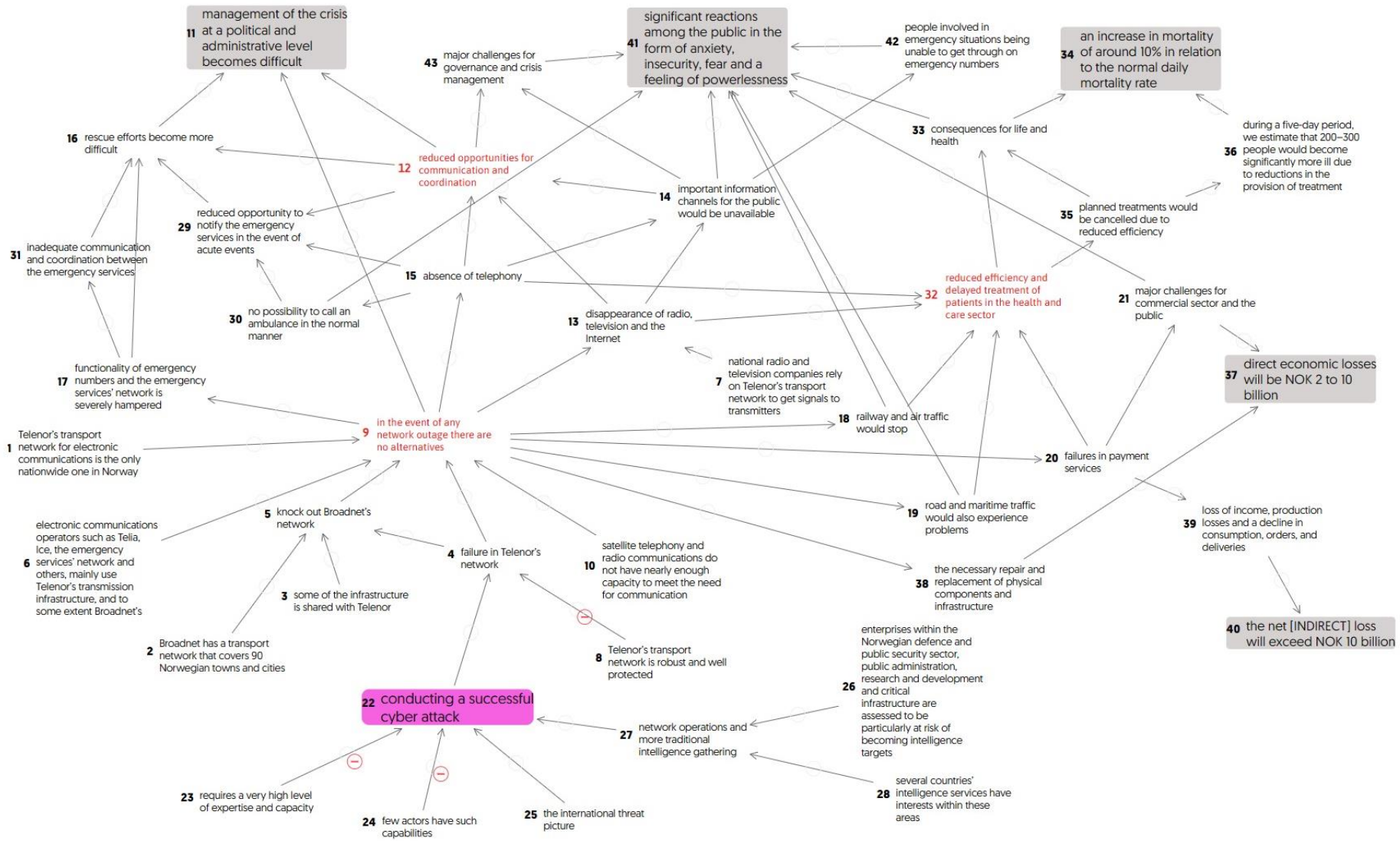

Figure 2 The complete risk model corresponding to Scenario 18.2.

Does the Basic Risk Model Exhibit Systemic Risk?

Systemic risk has a particular kind of complexity, viz., *dynamic complexity*. Dynamic complexity arises if there is causal feedback in a system (Sterman, 2000, p12-13, 138-141). In the case of disasters, one has reinforcing feedback of risks (vicious cycles of risks). Systems with vicious cycles have dynamic complexity, which makes them very difficult to manage (Eden & Gonzalez, 2003; Gonzalez & Eden, 2023).

A powerful feature of *Strategyfinder* is its ability to detect and identify feedback loops using analysis algorithms applied to the directed graph representing the risk model. Using this feature on the basic risk scenario model, *Strategyfinder* reported 'no loops detected'. Accordingly, the model of risks and their causal interconnections matching the description provided in (Norwegian Directorate for Civil Protection, 2020, p204-207) must be incomplete, since it does not have feedback loops and, hence, lacks major cascading effects. A massive cyber attack leading to a full failure of the electronic communication devices for five days in Norway must be expected to escalate the risks over time, i.e., to generate vicious cycles of risks (i.e., reinforcing feedback loops of risks and risk outcomes).

ACCOUNTING FOR SYSTEMIC RISK USING THE *STRATEGYFINDER* METHOD

We recall from the previous section, that scenario 18.2 described in (Norwegian Directorate for Civil Protection, 2020, p204-207) does not account for all the causal links among the listed risks, since the basic risk model does not have feedback loops. Without feedback loops the dynamic behaviour of the basic risk model appears to be far too simple. There is no escalation of risks over time. Such escalation must be expected as consequence of a massive cyber attack with cascading effects on several critical infrastructures.

In addition to the missing causal links, which must be expected within the critical infrastructures mentioned in (ibid, p204-207), viz. electronic communication, life and health, transport and finances, the description also seems to be incomplete regarding risks content. For instance, a massive cyber attack disrupting all electronic communication networks for five days would also knock out energy production, in particular hydroelectric energy production (Norway's main source of energy for the public, for much of its industry and for hospitals). Among the consequences of energy disruption, a major one would be the impact on livestock (cattle, pigs, etc), and fish farming (one of the main sources of Norway's prosperity), as well as the impact on refrigerators (household, commerce, and industry).

Extending the risk model to consider all aspects of a massive cyber attack is beyond the scope of this paper. (We mention in passing that such a full risk model would be needed in order to develop adequate mitigating strategies of the risks.) For the purpose of this paper, it is sufficient to show that a modest enhancement of the basic risk model generates vicious cycles of risks, with a resulting dynamic behaviour of risks escalation. In fact, we show that the escalation causes both inner-sector and inter-sector cascading effects.

Identification of Missing Causal Links and Their Consequences

Enhancing the basic risk model by adding a few more obvious causal links among the risks described in Scenario 18.2 'Cyber attack on electronic communications infrastructure' (Norwegian Directorate for Civil Protection, 2020, p204-207) generates several vicious cycles of risks.

To enhance the basic risk model, the third author of this paper, the crisis manager of the Kristiansand municipality, Norway, added causal links to the risk model. He has ample experience with *Strategyfinder* as he was lead participant for the Kristiansand municipality in the Systemic Pandemic Risk Management project 2020-2023 (Bryson et al., p24-30). The project used *Strategyfinder* and promoted a significant extension of the capabilities of the software. As champion of the approach, after the completion of the Systemic Pandemic Risk Management project, the crisis manager of the Kristiansand convinced the municipality to adopt *Strategyfinder* for systemic risk assessment and management.

On Fig. 3 the added causal links are shown as red arrows. The rational for the added causal links follows on p10:

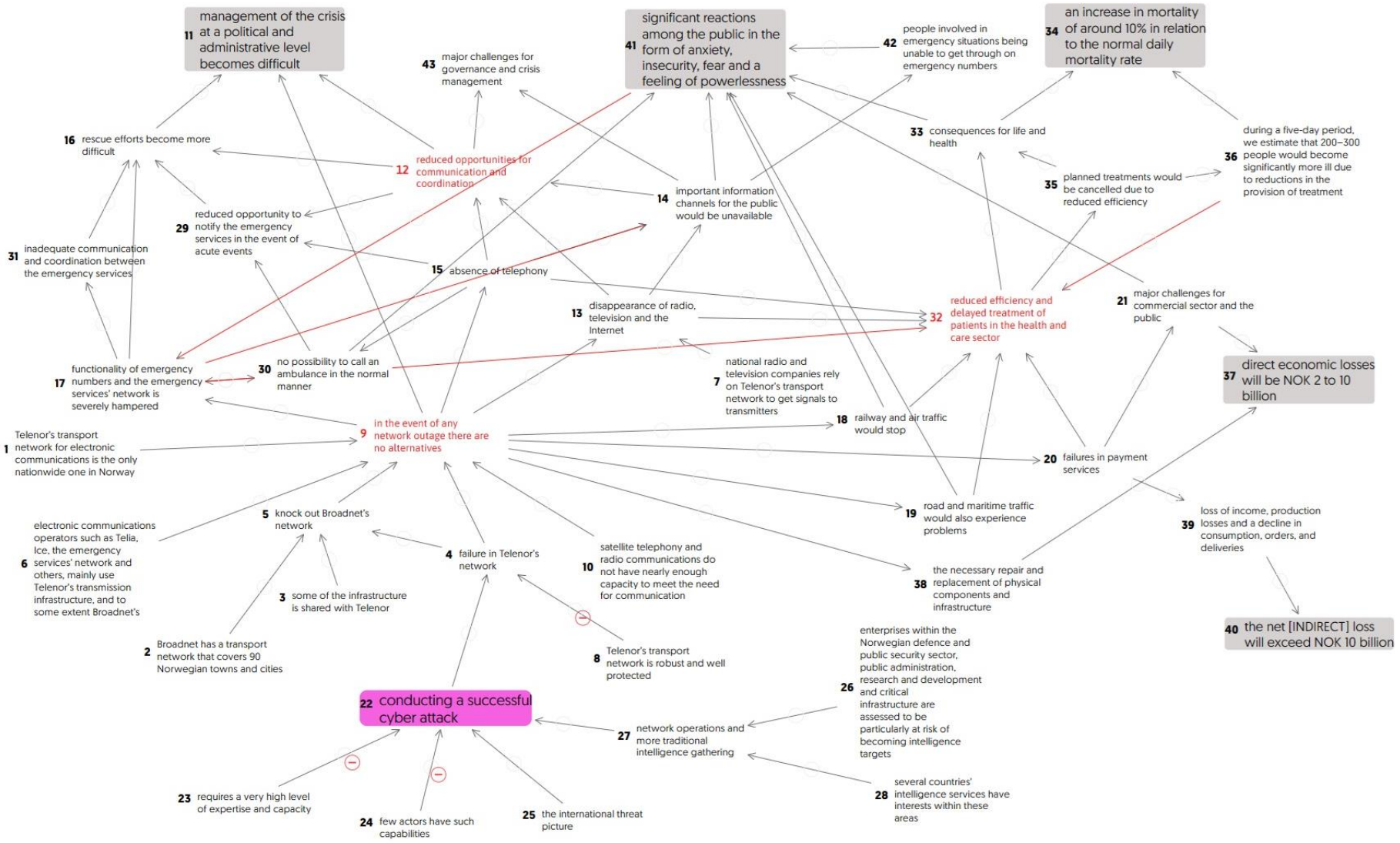

Figure 3 Risk model with added causal links (shown as read arrows). See the main text for the description of the added causal links.

ADDED CAUSAL LINKS AND THEIR EXPLANATION

- #17→30: The functionality of the rescue networks being severely hampered impacts on the ability to call an ambulance in the normal manner.
- #30→17: Not being able to call ambulances in the normal manner adds to the inconveniences hampering the functionality of rescue networks.
- #41→17: Significant reactions among the public (anxiety, fear, hopelessness) is likely to exacerbate conditions that may need request of rescue (which, lacking normal ways of communication, would often be delivered via messengers demanding attention from pressed rescuers).
- #30→32: No possibility to call ambulances impacts on the efficiency of treatment of patients and adds delays.
- #17→14: Since rescue services may detect conditions that demand alerting the public.
- #36→32: A significant increase in serious illnesses will reduce the efficiency treatments in hospitals and cause time delays

In the resulting risk model (Fig. 3), *Strategyfinder* detects 7 feedback loops, all acting as vicious cycles. Fig. 4 shows the result of the analysis.

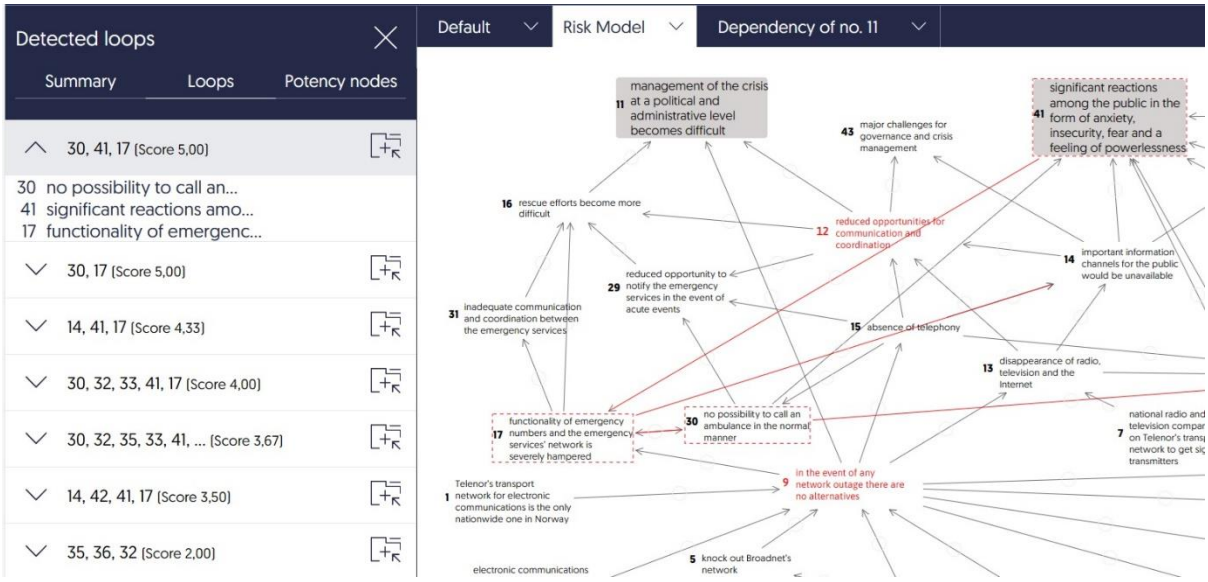

Figure 4 Detected feedback loops. Clicking on a detected loop (here, 17→30→41→17), selects the corresponding risk nodes on the risk model (shown in red colour framed with dashed lines).

We skip the explanation of the scores, since they are not relevant for the purpose of this paper (other than to comment that higher scores mean more potency of the risks).

The symbol to the right of the score indicates that clicking on it creates a new view and the view displays the corresponding loop.

Figure 5 shows the new view (labelled 'Loop 30,17') and the loop (vicious cycle) #17↔#30; note that #17 impacts on #30, and #30 impacts back on #17.

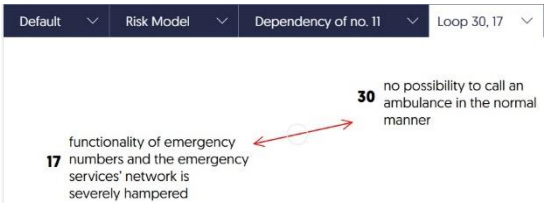

Figure 5 The loop #17↔#30. See main text.

Risk #17 belongs to the electronic communication infrastructure, whereas risk #30 belongs to the public health infrastructure. In other words, the vicious cycle #17↔#30 causes inter-sector cascading effects.

This loop #17↔#30 is part of 4 vicious cycles and the risk #17 participates as node in 6 vicious cycles.

Figure 6 is a composite figure where the 7 feedback loops detected by *Strategyfinder* in the enhanced risk model are shown.

Figure 6 The seven feedback loops in the enhanced risk model, each loop acting as a vicious cycle.

The loop labelled (a) on Figure 6 is identical to the loop #17↔#30. It was discussed in the previous page.

The loop labelled (b) is a nested loop, consisting of two single loops, viz. #30↔#17 and #30→#41→#17→#30, which share the node #17. In a nested loop, each of its components act as a single vicious cycle and the interaction between the single loops potentiates their impact. As in the case of the vicious cycle labelled (a), the vicious cycle labelled (b) causes inter-sector cascading effects. As mentioned earlier, risk #41 is likely to generate riots, affecting yet another critical infrastructure (security services). However, the scenario 18.2 does not mention this likely consequence.

The loop labelled (c) is the single loop #14→#41→#17→#14. This loop causes inter-sector cascading effects.

The loop labelled (d) is a nested loop, consisting of three single loops, viz. #30↔#17, #30→#41→#17→#30, and #32→#33→#41→#17→#30→#32. Alternatively, it could be described as consisting of the nested loop labelled (b) on Figure 6, and the single loop #32→#33→#41→#17→#30→#32. This loop causes inner-sector and inter-sector cascading effects.

The loop labelled (e) is also a nested loop. For simplicity, it can be described as consisting of the nested loop labelled (d) – which is itself nested – and the single loop #35→#33→#41→#17→#30→#32→#35. This loop causes inner-sector and inter-sector cascading effects.

The loop labelled (f) is also a nested loop. It consists of two single loops, viz., #17→#14→#41→#17 and #17→#14→#42→#41→#17. This loop causes inner-sector and inter-sector cascading effects.

Finally, the loop labelled (g) is a single loop: #32→#35→#36→#32. This loop causes inner-sector cascading effects.

Consequences for Mitigation Strategies

Unmitigated vicious cycles escalate the risks over time and increase the impact of cascading effects. Adding only five more obvious causal links to the basic risk model already generated 7 vicious cycles. If the basic model had been extended by adding more risks (e.g., risks belonging to the energy, the public security infrastructures and food) the number of vicious cycles would have risen significantly. A full extension of the basic model is out of scope. Notwithstanding, using the example below we can explain the principle for how to prioritise targets for mitigating strategies.

The straightforward answer is to target those risks which are in the most vicious cycles, the most potent risks. Figuratively speaking, killing as many birds as possible with one stone (Gonzalez et al., 2021).

Figure 7 displays the outcome of the *Strategyfinder* loop analysis.

The 'nodes' (the risks) in the model are evaluated regarding how many loops (here, vicious cycles) that would be killed by a successful mitigation strategy targeting the node (the 'potency' of the node).

The risk #17 has the highest potency, viz., 6.

Indeed, a glance at Figure 6 shows that #17 is in 6 of the 7 loops. Thus, a strategy mitigating that the cyber attack hampers the functionality of the emergency numbers and the emergency services will counteract the escalation driven by 6 vicious cycles.

Next, the risk #41 has potency 5.

Indeed, a glance at Figure 6 shows that #41 is in 5 of the 7 loops. Thus, a strategy mitigating that the cyber attack causes significant reactions among the public will counteract the escalation driven by 5 vicious cycles.

The reader can compare Figure 7 with Figure 6 and check that the potency of each risk appearing on Figure 7 always corresponds to the number of times the risk is part of a vicious cycle.

The *Strategyfinder* analysis tool reveals much more useful information for strategy development, such as dependencies of a node on other nodes (Fig. 1 is such an outcome), busy nodes (such as #9, #12 and #32) or negative goals (viz., #11, #34, #37, #40 and #41). As to negative goals, cf. p6. The interested reader finds the freely available manual 'Analysis Tools' on https://www.strategyfinder.com/.

Potency	#	Statement
6	17	functionality of emergency numbers and the emergency services' network is severely hampered
5	41	significant reactions among the public in the form of anxiety, insecurity, fear and a feeling of powerlessness
4	30	no possibility to call an ambulance in the normal manner
3	32	reduced efficiency and delayed treatment of patients in the health and care sector
2	33	consequences for life and health
2	35	planned treatments would be cancelled due to reduced efficiency
2	14	important information channels for the public would be unavailable
1	42	people involved in emergency situations being unable to get through on emergency numbers
1	36	during a five-day period, we estimate that 200–300 people would become significantly more ill due to reductions in the provision of treatment

Figure 7 The Strategfinder feedback loop analysis reports the potency of the risks (see main text).

DISCUSSION AND CONCLUSION

The 2019 Global Assessment Report on Disaster Risk Reduction strongly emphasizes the pressing need for a fundamental shift in approaches to managing systemic risk (UNDRR, 2019, p.44). A significant ongoing challenge remains in ensuring that research is not only conducted but also effectively utilized and applied (Boaz & Hayden, 2002).

A recent review by Oliver et al. (2022) focuses on identifying existing activities that engage with research and policy, as well as assessing the impact of these activities on both research outcomes and decision-making processes. The review concludes that many researchers have yet to successfully bridge the gap between scientific knowledge and practical application, resulting in what is described as a substantial and growing volume of unfocused activity, lacking in effectiveness (Oliver et al., 2022, p.704).

Similarly, a recent article by Reichstein et al. (2021) in the prestigious journal Nature emphasizes the importance of creating models that are not only comprehensible but also directly applicable to policymaking. Advocacy for research utilization in practical settings is deemed essential (Boaz & Hayden, 2002, p.440).

The research presented in this paper set out to investigate whether national civil protection agencies account for systemic risk in their national risk assessments. To the best of our knowledge, the approach used in our paper, strategy mapping, is the only one that demonstrably has achieved useable and used mitigation strategies of systemic risk (Gonzalez et al., 2021; Gonzalez & Eden, 2022; Abildsnes et al., 2023; Gonzalez & Eden, 2023; Eden & Gonzalez, 2023; Bryson et al., 2023). The approach uses participatory modelling involving stakeholders, mostly practitioners, experts from different relevant disciplines, and – very important for the implementation of the mitigation strategies – power brokers.

Surprisingly, two decades into the realisation of the systemic risk notion by the disaster risk reduction community, no evidence was found that systemic risk is accounted for in the national risk analyses presented in the OECD countries report (OECD, 2018). From a national security perspective, this might potentially represent a deliberate exclusion by national governments if they deem it sensitive to disclose a thorough analysis of national risks.

Nevertheless, the aim of conducting risk assessments by national civil protection agencies is arguably to 1) provide overviews to politicians and business leaders; 2) communicate risks to a wide audience; and 3) as input for exercises and emergency planning at a regional level. We believe that the importance of systemic risk is too significant to justify its omission in national risks assessments. Emergency planning at the municipal and regional level, where the first line of disaster response will be effectuated, must be detailed and specific. Considering that regional risk assessments must involve sectors with critical infrastructure according to their presence and role, omitting systemic risk assessment at the highest level (national) would hardly encourage consideration of systemic risk at the regional level.

The OECD report was published in 2018 and there is a possibility that systemic risk since has become an important part of national risks assessments in some of the countries covered by the OECD report. However, we doubt that systemic risk is sufficiently accounted for in national risk assessments. Our doubt is based on two facts.

First, the most recent report from the United Nations Office for Disaster Risk Reduction (GAR, 2022) acknowledges (ibid, p146) that little progress has been done in this regard over the three years period following the previous global assessment report (GAR, 2019). Arguably, if national risk assessments had employed a novel method to account for systemic risks, the GAR2022 authors would have noticed and reported it.

Second, Norway has not yet conducted *national* risk assessments accounting for systemic risk despite acknowledging its importance and the availability of relevant methods. The Corona Commission established by the Norwegian government in response to the COVID pandemic released a report (The Norwegian Corona Commission, 2020) stating that "In its emergency preparedness efforts, the Government has paid little attention to how risk in one sector is affected by risks in other sectors. A crisis preparedness system in which each sector evaluates its own risks and vulnerabilities, will fail if no one takes responsibility for evaluating the sum of the consequences for society at large. There is a need for a cross-sectoral system that can accommodate the interaction of risks across all sectors. This is a lesson applicable to preparedness in general".

Systemic risk assessment *has* been developed and applied in Norway recently, but then at the *regional level* in the Systemic Pandemic Risk Management project 2020-2023 using strategy mapping with *Strategyfinder*. The Systemic Pandemic Risk Management project included partners from the municipality of Kristiansand and the regional hospital (Bryson et al., p24-30), as well as international partners. Carefully selected stakeholders (both experts and decision-makers) participated in online workshops to create, analyse, and validate the risk model, to finally propose effective and practical mitigation strategies and identify roles to monitor and implement the strategies (Abildsnes et al., 2023, Bryson et al., 2023). Nonetheless, the Norwegian national authorities have not

yet adopted the method developed and applied at the regional level (in the Systemic Pandemic Risk Management project) for national risk assessments and mitigations strategies.

We mentioned several times that the purpose of strategy mapping is to develop strategies. But answering our research question did not require developing mitigation strategies. Our research question, whether national civil protection agencies account for systemic risk in their national risk assessments, only required examining 1) whether systemic risk was explicitly accounted for in the national reviews described in (OECD, 2018); 2) if there was evidence to that effect after 2018; 3) if there was evidence of feedback loops in a highly promising risk scenario 18.2 provided by the Norwegian Directorate for Civil Protection (2020).

The development of risk mitigation strategies for scenario 18.2 would have demanded a considerable extension of the risk model, i.e., it was out of scope.

On p2 we posed the question whether there is a fertile ground in future national risk assessments for using the recent advancements in strategy mapping. We hope to have created awareness that the method of strategy mapping for assessing and managing systemic risk originating in the field of complex project management deserve being adopted by the disaster risk reduction community.

Hence, we believe that the national civil protection agencies could significantly improve their risk analyses using strategy mapping to account for systemic risk. The report from the IBM Center for the Business of Government reviews strategy mapping (Bryson et al., 2023, p8-15, p41 and p43-46). The report also contains a section on the application of the Systemic Pandemic Risk Management project on mitigation strategies of systemic pandemic risk (ibid, p24-30). Finally, the report has an extensive comparison of different methods and tools for strategy mapping (ibid, p49-53).

CLARIFICATION

None of the authors has ownership in the *Strategyfinder* software and none of the authors is employed by the company owning the software.

REFERENCES

Abildsnes, E., Paulsen, S., & Gonzalez, J. J. (2023). Improving resilience against a pandemic: A novel technology for strategy development with practitioners and decision-makers. *Proceedings of the 20th International Conference on Information Systems for Crisis Response and Management*, Omaha, NE, USA.

Ackermann, F., Eden, C., Williams, T., & Howick, S. (2007). Systemic risk assessment: a case study. *J. Oper. Res. Soc.*, 58(1), 39-51.

Ackermann, F., Howick, S., Eden, C., & Williams, T. (2011). Delay and Disruption in Complex Projects. In R. A. Meyers (Ed.), *Complex Systems in Finance and Econometrics* (pp. 116-135), Springer.

Boaz, A., & Hayden., C. (2002). Pro-active evaluators – Enabling research to be useful, usable and used. *Evaluation*, 8(4), 440-453.

Bryson, J. M., Barberg, B., Carroll, A., C., E., George, B., Gonzalez, J. J., Rochester, J., Vandersmissen, L., and Zaki, B. (2023). Addressing Complex and Cross-Boundary Challenges in Government: The Value of Strategy Mapping. *The IBM Center for the Business of Government, Washington, DC, USA*. Retrieved February 5, 2024, from https://www.businessofgovernment.org/report/addressing-complex-and-cross-boundary-challenges-government-value-strategy-mapping.

Centeno, M. A., Nag, M., Patterson, T. S., Shaver, A., & Windawi, A. J. (2015). The Emergence of Global Systemic Risk. *Annual Review of Sociology*, 41(1), 65-85. doi:10.1146/annurev-soc-073014-112317.

Eden, C. Analyzing Cognitive Maps to Help Structure Issues or Problems. (2004). *European Journal of Operational Research*, 159(3), 673-686

Eden, C., & Gonzalez, J. J. (2023). The strategic management of disaster risk mitigation. In J. Radianti, T. Gjøsæter, & Y. Murayama (Eds.), *Information Technology in Disaster Risk Reduction ITDRR 2022*, (Vol. 672), Springer Nature.

Flood, S., Columbie, Y. J., Le Tissier, M., & O'Dwyer, B. (2022). Can the Sendai Framework, the Paris Agreement, and Agenda 2030 Provide a Path Towards Societal Resilience? In S. Flood, Y. J. Columbie, M. Le Tissier, & B. O'Dwyer (Eds.), *Creating resilient futures: integrating disaster risk reduction, sustainable development goals and climate change adaptation agendas*, Springer.

Gonzalez, J. J., Eden, C., Abildsnes, E., Hauge, M., Trentin., M., Ragazzoni, L., Berggren, P., Jonson, C.-O., and Abdelgawad, A. A. (2021). Elicitation, analysis and mitigation of systemic pandemic risks. *Proceedings of the 18th International Conference on Information Systems for Crisis Response and Management*, Blacksburg, VA, USA.

Gonzalez, J. J., & Eden, C. (2022). Insights from the COVID-19 Pandemic for Systemic Risk Assessment and Management. In J. Sasaki, Y. Murayama, D. Velev, & P. Zlateva (Eds.), *Information Technology in Disaster Risk Reduction ITDRR2021*, (Vol. 638), Springer Nature.

Gonzalez, J. J., & Eden, C. (2023). Devising Mitigation Strategies With Stakeholders Against Systemic Risks in a Pandemic. *Proceedings of the 20th International Conference on Information Systems for Crisis Response and Management*, Omaha, NE, USA.

Kaufman, G. G., & Scott, K. E. (2003). What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It? *Independent Review*, 7(3), 371-393.

Kim, Y.-k., Yoon, W. C., Lee, J., Poncelet, J.-L., Dolcemascolo, G., & Sohn, H.-G. (2022). A strategic response map for cascading pandemics: Lessons learned from the response to COVID-19 in the Republic of Korea. *Progress in Disaster Science*, 13, 100214. doi:https://doi.org/10.1016/j.pdisas.2022.100214

Lupton, D. (2013). *Risk* (2nd ed.), Routledge.

The Norwegian Corona Commision. (2020). *The authorities´ handling of the COVID-19 pandemic*. Retrieved 12th December 2023, https://www.regjeringen.no/contentassets/5d388acc92064389b2a4e1a449c5865e/no/sved/01kap02engelsk.pdf.

Norwegian Directorate for Civil Protection. (2020). *Analysis of Crisis Scenarios 2019*. Retrieved November 25, 2023, from https://www.dsb.no/rapporter-og-evalueringer/analyses-of-crisis-scenarios-2019/.

OECD (2018), *National Risk Assessments: A Cross Country Perspective*. OECD Publishing. https://doi.org/10.1787/9789264287532-en.

Oliver, K., Hopkins, A., Boaz, A., Guillot-Wright, S., & Cairney, P. (2022). What works to promote research-policy engagement? *Evidence & Policy*, 18(4), 691-713. doi:10.1332/174426421X16420918447616.

Reichstein, M., Riede, F., & Frank, D. (2021). More floods, fires and cyclones - plan for domino effects on sustainability goals. *Nature*, 592(7854), 347-349. doi:10.1038/d41586-021-00927-x.

Renn, O., Lucas, K., Haas, A., & Jaeger, C. (2019). Things are different today: the challenge of global systemic risks. *Journal of risk research*, 22(4), 401-415. doi:10.1080/13669877.2017.1409252

Schwarcz, S. L. (2008). Systemic risk. *The Georgetown Law Journal*, 97, 193-249.

Schweizer, P.-J. (2021). Systemic risks - concepts and challenges for risk governance. *Journal of risk research*, 24(1), 78-93. doi:10.1080/13669877.2019.1687574.

Sterman, J. D. (2000). *Business dynamics: systems thinking and modeling for a complex world*, Irwin McGraw-Hill.

UNDRR & UNU-EHS. (2022). *Understanding and managing cascading and systemic risks: lessons from COVID-19*. Retrieved Dec. 15, 2023, https://www.undrr.org/publication/understanding-and-managing-cascading-and-systemic-risks-lessons-covid-19.

United Nations Office for Disaster Risk Reduction UNDRR. (2019). *Global Assessment Report on Disaster Risk Reduction 2019 (GAR2019)*. Retrieved December 5, 2023 from https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2019.

United Nations Office for Disaster Risk Reduction UNDRR. (2022). *Global Assessment Report on Disaster Risk Reduction 2022 (GAR2022)*. Retrieved December 5, 2023 from https://www.undrr.org/gar2022-our-world-risk.

Williams, T. M., Ackermann, F., & Eden, C. (1997). Project Risk: systemicity, cause mapping and scenario approach. In K. Kahkonen & K. A. Artto (Eds.), *Managing Risks in Projects* (pp. 343-352), E&FN Spon.