J Transp Secur (2017) 10:45–62
DOI 10.1007/s12198-017-0178-5

Exploring vulnerabilities in preparedness – rail bound traffic and terrorist attacks

Veronica Strandh [1]

Received: 1 December 2016 / Accepted: 30 May 2017 / Published online: 22 June 2017

Abstract Railway and subway systems are regarded as being vulnerable to terrorism. This article examines different kinds of vulnerabilities in preparedness for terrorist-induced crises targeting rail bound traffic. Many discussions about critical infrastructures and their vulnerability to breakdowns and certain hazards are often discussed from the perspective of technical control systems or advanced mitigation efforts. This article contributes with another perspective. It is suggested that a wider perspective on what constitutes vulnerability is needed and the literature on disasters and crises is therefore informative. Relying on 20 interviews with actors from rail bound traffic and Sweden's crisis management system, the article focuses on different actors' own perceptions of their preparedness. The results show that the involved actors not only understand vulnerabilities in preparedness to be a matter of shortcomings in technical security systems or in the ability to secure trains from acts of antagonistic violence. Rather, they identify two additional significant vulnerabilities. First, increased organizational fragmentation in the sector is perceived as creating vulnerability in crisis management preparedness. Second, the failure to ensure that relevant actors have a cognitive and mental preparedness is seen as creating vulnerability.

Keywords Terrorism · Crisis management · Rail bound traffic · Vulnerability · Security · Public-private partnerships

Introduction

Scholars argue that society is becoming increasingly risk averse and vulnerable to different hazards (Beck 1992; McEntire 2004; Wisner et al. 2004; Renn et al. 2011). In particular, society is characterized by its interconnectedness, and our modern and often

✉ Veronica Strandh
veronica.strandh@umu.se

[1] Department of Political Science, Umeå University, SE -901 87 Umeå, Sweden

technically advanced systems are becoming increasingly vulnerable to breakdowns. Research has also shown that critical infrastructure systems, including communication and transportation systems, supply chains, and information technology and financial systems appear vulnerable to acts of terrorism (Boin and Smith 2006; Boin and McConnell 2007; Kapucu 2012). This observation merits further attention since society today is organized around essential functions such as transportation, food, and care.

This article explores different vulnerabilities in preparedness for terrorist-induced crises targeting a particular transportation sector, namely rail-bound traffic. The terrorist events in Madrid in 2004, London in 2005 and in St. Petersburg 2017 demonstrated the enormous consequences of a terrorist attack against rail-bound traffic, not only in terms of human suffering but also in terms of major disruptions in vital societal functions. In addition, print media has often reported on thwarted attacks, and railway and subway systems are in general regarded as being vulnerable to terrorism.

A paradox seems to exist. The observation that our society is more interconnected than ever leads one to assume that critical infrastructures require *unity* when it comes to their management. In terms of organization, however, we are now experiencing increased *fragmentation*. Rail-bound traffic is largely privately owned or operated, while there are no actors in society responsible for a systematic overview of critical infrastructures and the many different actors providing services of societal importance (Boin and Smith 2006; De Bruijne and Van Eeten 2007). Hence, the assessment of society's ability to deal with disruptions is becoming practically and methodologically challenging (Lindbom et al. 2015). In addition to this, a similar development can be observed in the security and crisis management environment (Olsen et al. 2007; Coppola 2011). In the effort to meet complex threats and enhance organizational capacity to respond to events such as terrorist-induced crises, governments at all levels are reaching out to engage actors from the private sector (Boin and Smith 2006; Rademacher 2014). Hence, another starting point for this article is the observation that the number of actors responsible for providing services of vital societal importance and which are assumed to engage in crisis management is on the rise. It is therefore becoming crucial to understand this development's implications for crisis management. By doing so, we can also better understand the role of the transportation sector in crises, an aspect which is overlooked by first responders and the transportation system itself (Edwards and Goodrich 2014).

There is no universal solution to the problem of how to organize crisis management in the context of terrorism targeting rail-bound traffic. The threat of terrorism varies among countries, and different parts of the world organize their rail-bound sectors differently. This article will concentrate on Sweden, which provides the empirical focus. On 7 April 2017, Sweden experienced a terrorist attack when a man drove a hijacked truck into crowds on a pedestrian street in Stockholm. The attack killed five persons and injured 15. This was the first terrorist attack in Sweden since the early 1970s. Accordingly, Sweden has relatively limited experience of dealing with terrorism and has yet to suffer a major attack on its rail bound traffic system. In theory, countries with prior experiences of responding to terrorism have learned lessons and developed mental and organizational preparedness. Turning to countries with less experience we can assume that the preconditions for bringing preparedness practices high up on the agenda are slightly different. Hence, Sweden, like other European countries, faces the precarious situation of having no or limited experience of dealing with a mass-casualty

attack on its transportation sector. Nonetheless, it must enhance its capacity to deal with potential disruptive events.

Preparing to deal with the challenges caused by terrorism is described as being a complex task (Hoffman 2006), and we can assume that preparedness processes are imbued with challenges and potential vulnerabilities. We can also assume that actors involved in preparedness have different levels of knowledge and resources and represent different views on what constitute vulnerabilities in their security and crisis management practices. Accordingly, taking on a vulnerability perspective and building on 20 interviews with rail-bound traffic actors and key players from the Swedish crisis management system, this article emphasizes the different actors' own perceptions of their current preparedness.[1] It is presented in four parts. First, it outlines the global trend lines concerning terrorist attacks targeting rail bound traffic and discussions about rail security. Second, it outlines the conceptual framework, presenting how we can analytically understand vulnerabilities from different perspectives. It gives special attention to the concept of vulnerability, which has gained momentum in disaster and crisis management research and is proposed as a useful concept when analyzing vulnerabilities of infrastructure systems and organizational capacity. Third, the different actors' perceptions of current preparedness practices are examined by asking the question *what preparatory efforts have been initiated in Swedish rail-bound traffic in order to recognize the threat of terrorism and prepare for the consequences of an attack.* It also raises the question of *what challenges and opportunities rail-bound traffic actors experience due to an increased institutional fragmentation.* Fourth, and in conclusion, vulnerabilities in the current system and practices are analyzed by answering the question of *what types of vulnerabilities have been identified in Swedish crisis management preparedness for terrorism targeting rail-bound traffic, and how these can be understood.*

Global patterns of terrorist attacks targeting rail bound traffic

The phenomenon of terrorist attacks targeting rail bound traffic is a *global* concern. Attacks occur in different parts of the world, and have done so since 1970, when terrorism began to be registered systematically in research databases (Strandh 2015). Hence, history has provided us with numerous examples of how passenger trains, freight traffic, stations and railway tracks have been targets of sabotage and different types of attacks. However, scholars argue that public transportation – rail bound traffic included – now also has become a target for terrorists whose goal is to cause *mass-casualty events* (Jenkins 2012; Waugh 2004; Strandberg 2013; Strandh 2015).

Analyzing attacks against rail bound traffic over a 40 years period, Strandberg (2013) shows that an overwhelming majority of the attacks since 1970 (1122 attacks in total) can be categorized as small ones that resulted in few casualties and limited infrastructure damage. Research also shows that terrorists tend to target *different* parts of the railway sector. Since 1970, 46% of the attacks have targeted parked or passing trains. Yet, 22% of all attacks have targeted stations and 17% have focused on railway tracks. Furthermore, one can observe a concentration of mass casualty attacks since 2001. Almost half of the 20 largest-scale attacks on rail bound traffic have taken place

[1] The 20 interviews were conducted before the recent terrorist attack in Stockholm on 7 April 2017.

since 2001. Hence, it has been a continuous increase in the number of people injured in terrorist attacks targeting rail bound traffic (Strandberg 2013).

As a consequence, how to secure rail bound traffic against terrorism has become a growing concern and researchers argue that more should be done to reduce risk on both passenger and freight rail. However, it is extremely challenging to secure the sector from antagonistic acts. Passenger profiling, metal detectors and security guards, all of which have become part of the landscape at airports, cannot be applied to rail bound traffic (Jenkins 2012). Meyer (2011) even argues that protective security measures should focus on *limiting* the damage caused by explosive attacks rather than on reducing the probability of an attack taking place. Accordingly, so called protective design is frequently discussed. Increased collaboration with architects and designers in order to improve station design is one example. Other security efforts include how to carry out random searchers of passengers and their luggage, increased presence of security officers and video surveillance as well as encouraging passengers to report suspicious activity.

Furthermore, and as indicated, rail bound traffic is an institutionally fragmented environment. We can compare to aviation which is also described as a fragmented environment, yet with a uniting and distinctive security culture. For example, there are many standards and regulations for international aviation safety and security. Similar institutionalized security mechanism do not exist for rail traffic (Andersson and Vedung 2010). Instead, initiatives to enhance security seem to vary across countries and the many different actors involved in railway traffic.

Understanding vulnerabilities through disaster and crisis research

It should be noted that much of the literature dealing with critical infrastructures and their different forms of vulnerabilities tends to focus on physical security, control systems, and how engineers can prevent breakdowns from taking place (Boin and McConnell 2007). Hence, vulnerabilities in transportation systems are often understood from the perspective of techniques and measures to mitigate inherent system vulnerabilities. This article contributes with another perspective. It is suggested that in the endeavor to explore vulnerabilities in preparedness for terrorist-induced crises on rail-bound traffic, a wider perspective on what constitutes vulnerability is needed. An entry point is the literature on disasters and crises, in which for example McEntire (2004, 2005, 2011) and Manandhar and McEntire (2014) has worked continuously on the topic of vulnerability.

Sudden-onset events tend to draw analytical attention to the dramatic event as such. However, a vulnerability approach goes beyond the triggering event and also pays analytical attention to the factors that contribute to harm and determine *proneness* to a hazard. Moreover, the vulnerability approach addresses factors determining management *capacity* when preparing for and dealing with the consequences of an event. In view of that, McEntire (2011:298) defines vulnerability as "a measure of proneness along with the ability to withstand or react to adverse consequences." His broad conceptualization relates to different research fields and their interpretations of the concept.

Traditionally, vulnerability has been discussed in relation to *natural hazards* such as earthquakes or hurricanes. A *geographic* or *engineering perspective,* understands vulnerability as emerging when structures and infrastructures cannot resist the forces

created by a given hazard. A *development perspective* stresses socioeconomic factors. For instance, the absence of land-use planning or use of low-quality construction materials, often in underdeveloped communities, accentuates vulnerability and the consequences of disaster events (Collins 2009). Furthermore, the *social vulnerability school* gives weight to how groups are differently affected by disasters in relation to factors such as gender, age, and disabilities (Britton 1986; Peacock et al. 1997; Pelling 2003; Wisner et al. 2004; Fordham 2004).

The traditional natural hazard paradigm is seen as ignoring man-made hazards, including terrorism and large-scale technical failures (Manandhar and McEntire 2014). In contrast, there are now scholars who emphasize vulnerability from such a perspective. Perrow (2007) states that terrorists' easy access to technology is one current concern. Taking a *complex-systems perspective*, vulnerability is understood as being created by the inbuilt dangers in the human–technology interface associated with today's interconnected systems (Perrow 2007). Vulnerability is also frequently discussed with a *homeland security* perspective in mind, in which the hazard terrorism primarily determines the degree of vulnerability proneness. At the same time, there is a realization that the potential sources of harm are so many that it is simply impossible to stop all antagonistic attempts. For that reason, vulnerability is also seen as produced by permeable borders, difficulties of protecting critical infrastructures, or ineffective counter-terrorism strategies (McEntire 2005).

From an *emergency management perspective*, the interpretation of vulnerability relates to the lack of organizational capacity among key responding actors to carry out their activities before, during, and after a crisis (McEntire 2005). From a *political science* perspective, vulnerability is produced by diffused political structures, inability to enforce regulations, and incorrect decision making, for instance due to unclear division of responsibilities among actors (McEntire 2005). According to scholars (McEntire 2004; Mileti 1999), people's and organizations' attitudes and behaviors are also significant determinants of vulnerability. At one end of the spectrum, organizations have a fatalistic perspective, seeing crises or disasters as an act of God, indicating a sense of passivity, while at the other end, organizations overestimate their capacity to deal with disasters (Clarke 1999).

Drawing on different fields of research, McEntire (2011) finds important intersections and concludes that the concept of vulnerability is a dual concept. This means that it encompasses two components, factors that determine proneness (which he calls *liabilities*) and factors that are associated with limited response capacity (which he calls *capabilities*). Four ways to reduce vulnerability emerge: reducing risk and reducing susceptibility (involving efforts that eliminate the variables that lead to crises) and increasing resistance and increasing resilience (including activities that can mitigate impact or react to the consequences of a crisis). Accordingly, vulnerabilities exist and require actions, before, during, and after a crisis.

For the purpose of this article, the main merit of a vulnerability perspective is how it enables a broad discussion on crisis management preparedness, in terms of both factors that determine vulnerability and factors that are experienced as limiting the response capacity. From our empirical perspective—that is, how Swedish actors prepare for responding to terrorism targeting rail-bound traffic—the vulnerability perspective draws attention to how the actors experience the risk of terrorism, obstacles to current crisis management practices, and measures to resist and recover from acts of

antagonistic violence. It thereby captures both dimensions of vulnerability: liabilities and capabilities.

Examining vulnerabilities

When exploring vulnerabilities in preparedness, some guidance can be found in national publications and in risk and vulnerability assessments that indicates that train and subways systems are likely targets for acts of terrorism and that the consequences could be far-reaching if an attack took place. In order to gain a more comprehensive picture, as well as to discern different perspectives among central actors, it is suggested that the involved organizations' own perceptions of their preparedness practices need to be examined. Therefore, as stated, empirically this article builds on 20 semi-structured interviews with rail-bound traffic actors and key players from the Swedish crisis management system. The role of the transportation actors in particular is considered, including the role of central rail operators and railway authorities: SJ AB, Green Cargo, A-Train AB, MTR Stockholm, Jernhusen, the Swedish Transport Administration, and the Swedish Transport Agency. Each interview was conducted by the researcher and lasted 60–90 min on average. An interview guide was sent out beforehand to the respondents so they could reflect upon what they regard as threats against rail-bound traffic, their particular institutional environment, and their crisis management practices. The respondents were specifically asked to reflect upon the capacity to prepare and respond to a scenario involving a mass-casualty terrorist attack.

Rail-bound traffic in Sweden—the threat of terrorism

Similar to other European countries, Sweden has experienced major reforms to its railway system since the late 1980s. Before the path to deregulation, Swedish rail traffic was more or less synonymous with the Swedish State Railways (SJ), a state-owned business administration with a monopoly position (Alexandersson and Hultén 2007:22). Following the deregulation process, SJ was turned into a train operating company, and public procurement by competitive tendering was made possible. The current railway environment can be described as a patchwork of actors. Still, the Swedish state remains responsible for infrastructure investments and maintenance and holds a central position in the system through its ownership of entities such as SJ AB (passenger traffic) and Green Cargo (freight traffic). There are also subsidiaries that operate train traffic in specific parts of the country. Moreover, there are companies operating which are partly owned or wholly-owned by international actors. The Association of Swedish Train Operating Companies lists as many as 17 companies running passenger traffic and 21 companies running freight traffic (ASTOC 2015). When taking real estate into consideration, additional actors can be added to the patchwork. The state-owned Jernhusen owns a significant number of train stations, and the Swedish Transport Administration is another key actor in this field. Moreover, the maintenance of the railway system is carried out by a significant number of contractors, including state-owned actors as well as international actors (SOU 2013:83, pp. 49–64).

The respondents in this study— that is, actors from rail-bound traffic and the crisis management response system—agree that rail-bound traffic must be considered a

vulnerable target for acts of antagonistic violence. At the least, terrorists could target a significant number of civilians in crowded and confined spaces. The open character of the railway systems is seen to cause proneness to attacks and to offer easy escape routes for perpetrators. The vulnerability also pertains to the fact that there are few actual security measures in place to prevent attacks from taking place. However, there exist measures aiming to limit susceptibility, such as camera surveillance, the presence of security personnel, and the use of open and well-lit spaces to make it harder for perpetrators to carry out their acts.

The respondents give weight to the fact that companies running passenger or freight traffic do not necessarily constitute the prime targets as such. However, in terrorists' attempt to cause far-reaching consequences and achieve extensive publicity, no one escapes the notion that an attack against rail-bound traffic must be, in the eyes of terrorists, an "effective" target. Despite such risk awareness, the respondents report a diverse portfolio of hazards in need of their attention, ranging from people stealing copper and youth gangs playing on the railway or sabotaging the railway tracks to more severe threats such as lone perpetrators threatening or attacking passengers on trains or at stations. At the end of this spectrum, we find the threat of terrorism. This is how two respondents reflected:

> "I would say that we are talking about terrorism more frequently today; however, not in a systematic manner. Rather, we talk about terrorism when particular events take place; for example, after the suicide attack on 'Drottninggatan' in 2010 or in connection with the Obama visit to Sweden." (interview 2)

> "I'm sure that it's not due to reluctance, it's that it's almost pedagogically impossible to introduce this way of thinking. Looking at our director general, he is on TV or radio every other day since it's about derailments and poor maintenance. What should I then do to start working with this?" (interview 4)

Even though terrorism is not perceived as being the most imminent threat to Swedish railroads, the respondents agree that it is realistic to believe that a major attack eventually will strike Sweden (as stated, the interviews for this article were carried before the very recent terrorist attack in Stockholm, 2017). The respondents described how there is a tendency among the actors to focus on challenges emanating from daily and more tangible safety and security concerns. Poor railway maintenance, recurring mishaps, derailments, poor punctuality and dissatisfaction over lack of passenger information are examples of topics that are frequently discussed in the media and in political circles. As a consequence, a vulnerability is seen emerging since less systematic attention (or a total lack of attention, according to some respondents) is paid to the threat of terrorism.

Organization of preparedness for terrorist-induced crises

An awareness exists that trains, train stations, railway tracks and subway systems appear vulnerable to different kinds of violence. The obvious question, then, is what

preparatory efforts have been initiated in order to prepare for managing the consequences of an attack.

Organization through preparedness tools

A comparison can be made between the types of organizations represented in the empirical material. The interviews held with first responders—that is, specialized crisis management organizations—revealed exercise-intensive environments, meaning that they practice on a regular basis. In combination with their regular exposure to emergencies, they develop a capacity to operate during chaotic and uncertain situations. The interviews conducted with rail authorities and rail operators revealed a different picture. They do not have the same mandate in crises as the first responders do, and this is echoed in the frequency and quality of resources and systematic attention given to crisis management. Hence, if we concentrate on the preparedness tools available for rail-bound traffic actors, one can begin by mentioning risk and vulnerability assessments. Each actor is obliged to carry out such analyses to gain knowledge about hazards, risks, and vulnerabilities within its own area of operations. Varying opinions can be identified among those respondents who emphasize the usefulness of their assessments, while others call attention to how it is challenging to carry out a solid assessment when it comes to terrorism. Their main critique resembles the fact that very limited information is provided about the actual threat picture, and there is limited knowledge about how to act if the national threat level changes.

Other preparedness tools include participation in workshops or in table-topic exercises. Such preparatory efforts tend to include a limited number of people with strategic positions and take place on average 1–2 times a year. If we look at preparedness initiatives that focus exclusively on the threat of terrorism, rail-bound traffic actors have participated in very few, if any, activities. A recent exception is a project initiated by the Swedish Transport Administration and Jernhusen that focuses on crisis situations at traffic hubs in the three largest cities in the country and in which the threat of antagonistic violence is included as a scenario. There are also joint exercises, called full-scale exercises; the last major joint exercise that focused on the threat of terrorism was held in 2007.

We can conclude from the interviews that the respondents call for a more systematic approach to knowledge building and exercises. In particular, the growing number of actors involved in rail traffic is seen as accentuating the need for an organized and systematic approach. It can be illustrated by the following citations.

> "There are some occasions when the Swedish Transport Administration has coordinated joint exercises. But this must be systematized and done more regularly. It should not be a one-time event that someone happens to realize is needed." (Interview 2)

> "In the railway system it doesn't matter how small you are; you can cause a big crisis for the whole system even if you only drive 20 trains per month, the same as if you drive 200 trains." (Interview 2)

One can discern uncertainties among the actors, and they raised questions themselves during the interviews. For example, when and how should the railway

family exercise? Should all actors be included in exercises? Can or should international owners or operators be forced to participate? The respondents are all central actors and they hold a significant share of today's market. Focal persons at these organizations know each other on a personal basis. They interact and share experiences, and the importance of trust was frequently mentioned. The challenge seems to revolve around the capability to bring together the different actors in the seemingly fragmented environment, and it was suggested that already established actors must better interact with smaller or newer operators on the market. As the citation above illustrates, a terrorist attack can strike a minor company as well.

Another point that was revealed from the interviews is the frequently used concept of *lessons learned* and how it implies a strong emphasis on ordinary and regularly occurring safety and security concerns. Some respondents underlined how a focus on experiences of already known hazards and events in the past might cause a vulnerability since it hampers the ambitions to reflect on and prepare for unforeseen situations in the future. There is concern that a behavior is developed in which a "crisis management in hindsight" culture exists. That is, one tends to focus on past experiences, and this creates a reactive rather than a proactive approach.

> "We had a scenario with a planned bomb, and that was pretty useful. But many people also felt that it was nothing useful to practice since it will probably never happen. But that's what one needs to practice, the thing that one still doesn't think will happen." (Interview 2)

> "We are so naive in Sweden, we think that nothing bad can happen to us." (Interview 4)

The perceived institutional pattern of focusing on well-known challenges was exemplified in the actual interview situations. Interviewees talked about their previous crisis experiences in terms of *highly critical situations* or even in terms of *extraordinary circumstances*. However, their exemplifications included trains having vehicle problems for a sustained period of time or different problems relating to harsh winter conditions. With respect for such situations being challenging and with implications for commuters, they are by no means of the same scale as a terrorist attack resulting in a mass-casualty situation or in a significant infrastructure breakdown.

Organization through collaboration

The provision of services in Swedish rail-bound traffic has shifted from being primarily an *intra*-organizational to an *inter*-organizational task. Also, the crisis management environment builds on the idea of collaboration across sectors, among different levels of government, and between public and private actors. It is not surprising that respondents all express resounding support for enhanced inter-agency relations. As one respondent declared, "there is no competition when it comes to security and crisis management." However, it is noteworthy that actors have very different interpretations of how collaborative actions are supposed to be performed.

It was mentioned during several interviews that the antagonistic dimension of the hazard was perceived as adding an extra layer of complexity to collaborative actions. When organizations prepare for or discuss their capacity to respond to terrorism, particular organizational intersections emerge. Hence, working with reducing the risk of terrorism or managing its consequences requires collaboration between intelligence and police authorities, specialized crisis management actors, and rail-bound traffic actors. The rail-bound traffic actors explained how they are used to working in networks that usually revolve around matters relating to information and control systems or weather-related situations. In such known situations, they know who to contact and involve in the process. However, in a specific terrorism context, the situation is different. What stands out is a recurring reflection that information flows and inter-agency relations in relation to intelligence and police authorities are not as defined, owing to the sensitive character of intelligence information and different organizational cultures. This is how some respondents reflected:

> "In Sweden we don't have real clarity. What does this network look like? What does the connection to the police authorities look like, then down to the Swedish Transport Administration and then on to the actors?" (Interview 2)

> "The preparedness is good but not sufficiently initiated within this specific area. There is a network based on the fact that we are a small country where most people know each other and those working on security have their branch colleagues' mobile phone numbers. If something happens, the alarm chain will be activated, but it's then built more on a personal commitment rather than a proactive collaboration and a systematic way of working." (Interview 1)

The respondents gave voice to an uncertainty about how they are assumed to work with matters relating to security and terrorism. Above all, there is no common ground for how the preparedness process should look or how high the level of ambition should be. After all, there are other hazards and challenges that divert attention.

> "What is needed is a statement that clearly outlines that we at least have a moral obligation to work with these issues. They must be put on the agenda, from the authorities' side. . . . There is no actor that believes that these issues don't need work, but the absence of attention "von oben" can cause it to not be at the top of the agenda. . . . The absence of terrorist events in Sweden in combination with a deregulation of rail-bound traffic is probably what causes this uncertain situation." (Interview 5)

One of the most surprising results we can see from the interviews is the very profound ambiguity of what authority the respondents consider responsible for managing collaborative efforts to enhance preparedness for terrorist attacks targeting the railway system. Two government agencies, the Swedish Transport Agency (responsible for railway safety supervision) and the Swedish Transport Administration (which owns and is responsible for maintenance and long-term

infrastructure planning for the railroads) were mentioned most frequently. At the same time, other authorities were mentioned, including the Swedish Civil Contingencies Agency (responsible for crisis management), the Swedish Security Service (responsible for counter-terrorism), and the Ministry of Enterprise, Energy and Communications (responsible for infrastructure and transportation). Most clearly, a vagueness exists about the division of responsibility between the Swedish Transport Agency and the Swedish Transport Administration. We can therefore conclude that no authority seems to hold exclusive oversight of security-related matters and preparedness for the specific threat of terrorism targeting rail-bound traffic.

Organization through response activities

If a terrorist attack strikes, first responders will be at the center of the response network, carrying out rescue efforts with the aim to save lives. The interviews with emergency personnel showed how they have well-defined roles and procedures, yet a terrorist attack on rail traffic is anticipated to be very demanding in terms of resources. The point here is that when it comes to other actors, such as a train company whose train becomes a target for a bomb explosion, the role of that company in the acute crisis situation is not as defined. Accordingly, during the interviews, each respondent was asked to describe what he or she envisaged as his or her main task if an attack took place.

> "We don't cut open any trains or carry people out. It's better that those who have practiced it can do it their own way. If they want help from us, we're there. . . . When the situation gets under control, then we can assist with buses or help out in other ways." (Interview 1)

Respondents anticipate their tasks to include taking care of lightly injured passengers, assisting at evacuations by providing resources such as buses, or providing meeting places for passengers and their relatives. They further stress their role as being about information sharing and supporting first responders. On this note, and from the perspective of first responders, the message is that the transportation actors need to know their roles, mandates, and resources in order to participate in a response successfully. They must be prepared to work under conditions of significant stress. This how two first responders reflected:

> "They (the train operators) have to create an organization for this so they know what role and mandate they actually have …. When we have established a command site, we want to see a representative from the affected company, and this person needs to know its mandate. So they can provide us with assistance and vice versa." (Interview 10)

> "The police, emergency medical personnel, and firefighters know their roles and responsibilities and are more or less prepared to respond to any kinds of

> scenarios, but other actors we collaborate with are not as experienced with handling chaos and might not have such a capacity." (Interview 3)

Respondents anticipate severe challenges when it comes to providing the public with information. If a terrorist attack targets an urban railway infrastructure, it means that the public transportation will be shut down, leaving thousands of stranded passengers. How to communicate information in such a chaotic situation becomes a key challenge. The communication aspect also applies to internal communication in the different rail companies as well as among actors in the railway sector. A prompt activation of crisis management plans and functions, information for employees, and strategic decisions for future actions requires effective information flows. As a result of trust-building and close relationships between focal points at different major organizations, most interviewees feel confidence regarding whom to contact in case of a major crisis. However, the system is considered vulnerable to a technical communication breakdown. A concern exists that certain important nodes, such as the Swedish Transport Administration, will quickly be overloaded in case of a terrorist attack.

Organization and societal responsibility

A terrorist attack on a central transportation system could result in many casualties as well as major infrastructure damage, not least because interconnected system are perceived as having the potential to cause cascading effects. Hence, the interviews revolved around discussions about major societal crises, and it is notable how frequently respondents referred to the term "society."

> "We will soon face a situation when we stay passive; instead, the society takes action and handles the situation, at least the first 12-48 hours." (Interview 1)

> "I don't say that I don't care if it's a terrorist attack or not, but it is not our work to make that analysis and worry about it. We should do our work within our own area of operation, and other actors, other authorities, and the society at large should take care of the crisis." (Interview 19)

Put simply, it is assumed that a societal crisis will be managed by the society. Respondents expressed their confidence in society's combined resources being capable of managing a major crisis. However, the definition of society or how actions are to be carried out is not entirely clear. On this note, one rail operator suggested that there is a need for a shift in focus. On a daily basis, providers of rail service or other services of critical importance have their main attention directed toward their passengers or clients. For the rail traffic sector it is all about transporting passengers as effectively and safely as possible. However, in times of crisis, the respondent proposed, there is a mounting need for transportation actors to expand their focus from just concentrating on passengers to also thinking in terms of a societal perspective. That is, they must have the capacity to adapt to the situation and have enough resources to work effectively under chaotic circumstances for a long period of time and resume operation as soon as possible.

However, many rail-bound traffic actors have limited experience dealing with actual prolonged crises.

> "We have never experienced any crisis that has lasted more than a couple of hours or maximum half a day." (Interview 12)

> "Our disaster management preparedness has never been activated or really tested.. .. There are cases when we have taken a proactive role and had standing stand-by, but then the situation has developed in such a way that it has not required any further actions.. .. More frequently occurring railway incidents are in one way easier to manage. You can stop and say, 'let's take a break here for 12 hours and rest.' Then you can return the following day. But with a scenario like this, with a terrorist attack, we do not have that opportunity and that is the big difference." (Interview 5)

Aspects such as resources, adaption, endurance, an ability to bounce back, and improvisation are all typically associated with the idea of resilience. This critical aspect of crisis management was in various ways emphasized by the respondents. There is a realization that a crisis with significant societal impact requires resilient organizations. However, constraints to resilience are easily identified, and minor companies have very few resources and little manpower to act in what can be described as a resilient manner. Financial resources also come across as a main constraint for governmental transportation authorities. The interviews clearly indicated that a resilient approach to complex threats is hampered by everyday demands on efficiency. Rail-bound traffic actors, government authorities, and specialized emergency organizations all face scarce resources and slim organizations.

Fragmentation—Potential implications

Changes on a societal level, including deregulation processes, have profoundly changed the preconditions for the ownership of critical infrastructures. As mentioned, Swedish rail traffic has experienced major reforms since the late 1980s and consists today of a high number of different stakeholders.

One line of reasoning that emerged in the interviews is the conviction that a fragmented rail environment cannot be considered negative for crisis management preparedness, per se. It was suggested that the ever-increasing number of train operators means more actors working dedicated to security. In addition, a few respondents stated that they think the complexity that is often attributed to rail traffic in Sweden is exaggerated. A second way of reasoning was expressed by those respondents who were keener to address the challenges emanating from current fragmentation. The two lines of reasoning can be exemplified below.

> "The railway sector looks very different today, but I think we are starting to find our ways of working. At least in those groups and networks I participate in. I can

see an increased willingness to collaborate and to better understand other actors and their different activities." (Interview 6)

"The first thing you will discover when you pick up your contact list and try to make a call to another actor is that your contact information is outdated. That is frustrating. A common saying is 'every week there is a new rail operator.'" (Interview 5)

The fragmentation manifests itself through new interagency patterns, with new companies, contractors, and consultants coming onto the market. Moreover, since the deregulation path was initiated, repeated reorganizations have taken place within government authorities. The many changes are perceived by some respondents to cause vulnerability since they make long-term planning and solid knowledge building more difficult.

"We have been busy with different reorganizations since 1988. There are constant changes and never time to find some stability. . . . We should be lucky that there are a few key persons left with very important knowledge and long experience in this field." (Interview 1)

Public–private partnerships are seen by the authorities as the preferred way forward to reduce vulnerabilities and enhance crisis management capacity. What becomes interesting is that such collaboration to a large extent builds on trust or good will. In other words, there is little regulation of private actors' role in crisis management. The Swedish Civil Contingencies Agency states that public authorities have the main responsibility for societal security, but at the same time, "companies should be informed about threats and risks and are expected to participate in public–private partnerships" (MSB 2010:10). Accordingly, the interviewees were asked to reflect on what requirements, tools, and mechanisms are in place to prepare them for their expected participation in crisis management.

"You need a safety certificate, so you can say that it is included in the current safety supervision already. But I do have a feeling that safety certificates and current supervision is about how you can handle, let's say, a, derailment in rural Långsele and not about your capacity to work with crisis scenarios, exercises, or crisis management trainings from a broader systematic perspective." (Interview 5)

From the perspective of rail operators, there are several safety and security requirements in place, most notably the ones posed by the Swedish Transport Agency. The transportation of dangerous goods in particular is clearly regulated by law. However, a perceived weakness in current practices is the actual supervision, the way it is performed, and the extent to which it takes the broader crisis management capacity into consideration. A comparison to neighboring Norway was made by one respondent.

"Norway is very precise and it formulates clear safety requirements, while our authorities in Sweden carry out supervision on a more general systemic level.

> Sweden also has fewer resources than Norway. In Sweden they pose the question, do you have a training plan? –Yes, ok, that's good. This can be compared to Norway, where they really perform a detailed supervision, looking in detail how you train." (Interview 1)

Since public transport authorities can procure public transport services under competition, the actual procurement process was given attention.

> "I would like to see an improved competence when it comes to procurement processes. Now you tend to think from the perspective of how actors are able to function during normal circumstances. But what happens if something goes wrong? What if they cannot manage situations that differ from daily routines?" (Interview 14)

Today, quality in rail-bound traffic is primarily understood in terms of departures carried out, punctuality, information, and staff behavior. Hence, much revolves around an actor's capacity to function well during normal circumstances. From a security and crisis management perspective, however, the challenge lies in how to make sure that the same actor is prepared to handle situations outside normal routines.

Identifying and understanding vulnerabilities

This article set out to explore vulnerabilities in the preparedness for terrorism targeting rail-bound traffic. The general picture of rail-bound traffic being almost inherently vulnerable to man-made crises such as terrorism has been confirmed. There are several security vulnerabilities due to the open character of the railway system, and there are few security measures in place that could reduce the risk of antagonistic acts. It is highly difficult to develop structures that could resist the forces of an attack. In addition to these security vulnerabilities, we can now conclude that the empirical material has revealed two main vulnerabilities in the preparedness for terrorist-induced crises on train and subway systems.

First, increased organizational *fragmentation* is perceived as causing a vulnerability to crisis management preparedness. It has been established that the many railway operators, rail authorities, owners of infrastructure, contractors for maintenance or infrastructure, etc., constitute a patchwork of actors. This development was not perceived by all respondents as causing a vulnerability, per se. However, when such fragmentation—a continuous rise in actors—is combined with a lack of overview or lack of management, it indeed turns into a vulnerability with implications for security and crisis management.

The fragmentation manifests through unclear division of responsibilities among the actors. It has become apparent that transportation actors experience uncertainty about how they should prepare. This causes vulnerability in their preparedness capacity since no one knows how high the preparedness level for terrorist-induced crises should be or whether it should be given attention at all. Hence, a vacuum emerges in actual systematic preparedness activities. When turning to governmental authorities for guidance on how to prepare,

there is a marked confusion over whether actors should turn to the Swedish Transport Agency, the Swedish Transport Administration, or some other authority. Results from the interviews indicate that there is no coherent overview of the railway sector today, and once again, vulnerabilities emerge. The preparedness capacity is limited due to a lack of a *systematic* approach to preparedness activities, both in terms of preparedness tools such as joint exercises and the actual supervision of crisis management capabilities. In particular, this article has demonstrated that there is no systematic preparedness for the particular hazard of terrorism. As a rail actor, one talks about terrorism, or practices terrorist-induced situations, only occasionally or not at all.

Second, a lack of *cognitive and mental preparedness* is seen as causing vulnerabilities in current crisis management practices. At the beginning of this article, it was suspected that a country with limited experience of dealing with major terrorist-induced crises might face particular challenges in the preparedness process. On the basis of the empirical material, we can confirm this assumption. The lack of experience makes it challenging for actors to make sense of diffuse threats and turn risk awareness into preparedness actions. In the interviews, it was put forth that Sweden seems to have a reactive approach to truly major crises. Some even described Sweden as being naïve or in denial of actual security changes taking place.

A related point to the perceived lack of a cognitive and mental preparedness is the transportation sector's unfamiliarity with highly chaotic situations. Terrorist attacks are foremost associated with law enforcement, fire service, and emergency medical services. However, this article has revolved around how rail-bound traffic actors increasingly, through private–public partnerships, for example, are assumed to take an active role when societal crises occur. An identified vulnerability is therefore the transportation sector's unfamiliarity with working in chaotic crisis settings, even though they are assumed to operate in the more peripheral parts of a response following a terrorist attack. Their role adheres foremost to avoiding a transportation breakdown and alternatively to resuming operation as soon as possible. However, they nevertheless need to know their mandate and resources and have an understanding of the procedures that goes beyond daily operation.

Different vulnerabilities have now been identified, and some reflections on how to analytically understand them are in order. It emerges that no single perspective upon vulnerability captures the complexity associated with preparedness for terrorist-induced crises. We can recall the observation that many discussions about critical infrastructures and their vulnerability to breakdowns and certain hazards often are discussed from the perspective of technical control systems or advanced mitigation efforts. Furthermore, a traditional perspective in the disaster literature understands vulnerability through the lens of a particular hazard or as the likelihood that a crisis will occur. Using McEntire's (2011) terminology, *liabilities* are then the focus of attention, and this perspective was partly echoed in the empirical material that discussed the difficulty of protecting the railway system from attacks. However, the two other main vulnerabilities, increased organizational fragmentation and lack of cognitive and mental preparedness, suggest that other understandings and perspectives on vulnerability also matter. One can stress McEntire's conceptualization of vulnerability as being a dual concept, understood in terms of both liabilities and capabilities. Hence, the two main vulnerabilities identified adhere to organizational *capabilities*; that is, many challenges in current

preparedness relate to actors' actual preconditions to carry out their activities, their organizational behavior, and their attitudes. This is an important observation since how actors invest, prioritize, and organize their preparedness is something they can actually try to control and enhance.

It is much harder for actors to control the actual hazard or risk of a threat becoming a real crisis. This calls for further studies of the role of transportation actors when it comes to preparedness for terrorist-induced crises. They are expected to take on an active role in crisis management, yet in this case, it appears there are few practices in place to prepare them for such a demanding task.

References

Alexandersson G, Hultén S (2007) The Swedish railway deregulation path. Rev Netw Econ 7:18–36

Andersson M, Vedung E (2010) Säkerhet och avvägningar i de fyra trafikslagen. Uppsala, eCajoma Consulting. Available from: http://www.cajomaconsulting.se/sakerhet.pdf. Accessed 20 Jan 2015

ASTOC - Association of Swedish train operating companies. Medlemmar http://www.tagoperatorerna.se/medlemmar_3. Accessed 20 June 2015

Beck U (1992) Risk society - towards a new modernity. Sage Publications, London

Boin A, McConnell A (2007) Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. J Conting Crisis Manag 15:50–60

Boin A, Smith D (2006) Terrorism and critical infrastructure: implications for public-private crisis management. Public Money Manag 26:295–304

Britton N (1986) Developing an understanding of disasters. Aust N Z J Sociol 22:254–271

Clarke L (1999) Mission improbably: using fantasy documents to tame disasters. Chicago University Press, Chicago

Collins A (2009) Disaster and development. Taylor & Francis, New York

Coppola D (2011) *Introduction to International Disaster Management*, 2nd ed. Butterworth Heinemann, Amsterdam

De Bruijne M, Van Eeten M (2007) Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. J Conting Crisis Manag 15:18–29

Edwards F, Goodrich D (2014) Exercise handbook: what transportation security and emergency preparedness leaders need to know to improve emergency preparedness. Mineta Transportation Institute, San José

Fordham M (2004) Gendering vulnerability analysis: towards a more nuanced approach. In: Bankoff, Frerks, Hillhorst (eds) Mapping Vulnerability: Disasters, Development and People. Earthscan publications, London, pp 174–182

Hoffman B (2006) Inside Terrorism. St. Andrew's University Press, London

Jenkins B (2012) The transportation threat to surface transportation: the challenges of securing public places. In: Kamien D (ed) The McGraw-Hill Homeland Security Handbook: strategic guidance for a coordinated approach to effective security and emergency management. McGraw Hill, New York, pp 21–31

Kapucu N (2012) Network governance in response to acts of terrorism: comparative analyses. Routledge, New York

Lindbom H, Tehler H, Eriksson K, Aven T (2015) The capability concept -on how to define and describe capability in relation to risk, vulnerability and resilience. Reliab Eng Syst Saf 135:45–54

Manandhar R, McEntire D (2014) Disasters, development and resilience: exploring the need for comprehensive vulnerability management. In: Kapucu N, Liou TK (eds) Disaster and development: examining global issues and cases. Springer, New York, pp 19–37

McEntire D (2004) Development, disasters and vulnerability: a discussion of divergent theories and the need for their integration. Disaster Prev Manag 13:193–198

McEntire D (2005) Why vulnerability matters exploring the merit of an inclusive disaster reduction concept. Disaster Prev Manag 14:206–222

McEntire D (2011) Understanding and reducing vulnerability: from the approach of liabilities and capabilities. Disaster Prev Manag 20:294–313
Meyer S (2011) Aiming for mass killings: explaining terrorists' selection of targets. Institute of Transport Economics, Oslo
Mileti D (1999) Disasters by design: a reassessment of natural hazards in the United States. Joseph Henry Press, Washington DC
MSB-Swedish Civil Contingencies Agency (2010) Krishantering för företag https://www.msb.se/sv/Produkter–tjanster/Publikationer/Publikationer-fran-MSB/Krishantering-for-foretag/. Accessed 10 Apr 2014
Olsen OE, Kruke BI, Hovden J (2007) Societal Safety: Concept, Borders and Dilemmas. J Conting Crisis Manag 15:69–79
Peacock W, Morrow B, Gladwin H (1997) Hurricane Andrew: ethnicity, gender and the sociology of disaster. Routledge, New York
Pelling M (2003) The vulnerability of cities: natural disasters and social resilience. Earthscan Publications, Sterling
Perrow C (2007) The next catastrophe: reducing our vulnerabilities to natural, industrial and terrorist disasters. Princeton University Press, Princeton
Rademacher Y (2014) Whole community: local, state, and federal relationships. In: Trainor J, Subbio T (eds) Critical issues in disaster science and management: a dialogue between researchers, pp 9–28 FEMA
Renn O, Klinke A, van Asselt M (2011) Coping with complexity, uncertainty and ambiguity in risk governance: a synthesis. Ambio 40:231–246
SOU - Swedish Goverment Official Reports 2013:83, *En enkel till framtiden? Delbetänkande av Utredningen om järnvägens organisation*. Stockholm: Ministry of Enterprise, Energy and Communication, 2013
Strandberg V (2013) Rail bound traffic—a prime target for contemporary terrorist attacks? J Transp Secur 6(3):271–286
Strandh V (2015) Responding to terrorist attacks on rail bound traffic challenges for inter-organizational collaboration. Department of Political Science, Umeå University, Dissertation
Waugh W (2004) Securing mass transit: a challenge for homeland security. Rev Policy Res 21:307–316
Wisner, Ben, Piers Blaikie, Terry Cannon and Ian Davis, At Risk: Hazards, People's Vulnerability and Disasters, 2nd ed. Boca Raton: Routledge, 2004