Chapter 7
Risk Management of Critical Logistical Infrastructures: Securing the Basis for Effective and Efficient Supply Chains

Michael Huth and Sascha Düerkop

1 Introduction

In summer 2017, parts of the railway network close to the German town of Rastatt sagged due to construction works for a new railway tunnel. Consequently, the route between Karlsruhe (Germany) and Basel (Switzerland) had to be fully closed for a duration of almost two months for both passenger and cargo transportation. The affected section of the railway network is a critical infrastructure for logistics: every day, approximately 200 cargo trains pass this link that connects Germany, the Netherlands, and Belgium with Switzerland and Italy. For those cargo shipments, the closure meant a severe problem. Some of the trains could be redirected, if bypasses were available and offered enough capacity; some trainloads could be transferred to road transportation or shipped on inland waterways. However, many shipments were put on hold and could not be delivered as planned. The activities to ease the problem led to an estimated additional cost for the railroad companies (excluding Deutsche Bahn) of almost 100 million EUR (Heinrici 2017). DB Cargo, a subsidiary of Deutsche Bahn, claimed lost revenues of another 46 million EUR (Schlesiger 2017).

This example shows that the logistical infrastructure plays a vital role in many developed countries for enabling both effective and efficient logistic chains. If one or more elements of the logistical infrastructure network are—even temporarily—not useable, logistic chains can be heavily affected. Thus, parts of the logistical infrastructure can be called critical.

M. Huth (✉) · S. Düerkop
Department of Business, Fulda University of Applied Sciences, Fulda, Germany
e-mail: michael.huth@w.hs-fulda.de

S. Düerkop
e-mail: sascha.dueerkop@w.hs-fulda.de

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_7

Possible events, that could lead to damages of the critical infrastructure (and consequently to additional cost) and threaten the economy of a county, will be stated as risks. Risk management, therefore, aims to identify, analyze, and evaluate risks as well as to develop and implement counteractive measures that should lead to a reduction of the probability of a risk and/or its consequences.

Risk management can be characterized by a closed loop of phases. The risk management loop can have the form of the iterative phase concept described in ISO 31,000. This article will focus on a specific step of the risk management loop: the risk evaluation. This phase aims to quantify previously identified risks so that they can be sorted by priority. Top priority risks are then managed immediately, whereas the management of low-priority risks might be postponed to a later stage. Thus, the risk evaluation leads to the recognition of the important and the less important risks.

In this article, we will develop an approach to how risks in logistical infrastructures can be evaluated. This should enable decision makers in risk management to make better (i.e., more justified) decisions and prioritize counteractions. We will start by giving examples for risks that can apply for critical logistical infrastructures following the PESTLE approach. We will then develop the evaluation approach, specify implementation aspects, and discuss its strengths and weaknesses as well as options to extend the approach. The chapter will be completed by a summary and an outlook on further research directions.

2 Risks for Critical Logistical Infrastructures

To ensure that all different fields of possible risks are thoroughly covered and systematically considered, a political, economical, social, technological, legal, and environmental (PESTLE) approach is used in the following. By investigating the keywords defined by the PESTLE abbreviation, it is ensured that no major possible risk factor is completely ignored or rejected. Albeit a completely qualitative approach, it serves as a capable method to give a first picture of the vast variety of risks the logistical infrastructure is typically exposed to.

Political risks are usually diversified into two separate sub-categories: macro-political and micro-political risks (Sottilotta 2013). While macro-political risks are not directly linked or directed to the affected business sector, namely the logistical infrastructure, micro-political risks are exactly that.

Macro-political risks, which can severely affect the logistical infrastructure, are all kinds of armed conflicts, including but not limited to full-scale wars, guerilla wars, and terrorism. In such volatile turmoil, infrastructural nodes and links, such as bridges, tunnels, train stations, or airports, are often either collateral damage or strategically targeted by bombing or other armed aggression. Recent examples include the Donetsk International Airport (Ukraine Today 2015), which has been defunct since mid-2014, the complete destruction of all bridges across the Euphrates River in the Syrian governorate of Deir ez-Zor (Zaman and Alwsl 2016), which were bombed by a US-led coalition air strike, or the Port of Aden, which was closed

down for months during the years 2016 and 2017. Furthermore, terrorist attacks deliberately targeted populated parts of the logistical infrastructure to maximize the effect of their actions, as the terrorist attack in Brussels 2016 (McKenzie 2016), which affected the tram service and airport of the city, showed to devastating effect. Other forms of macro-political risks through terrorism include maritime terrorism, such as the piracy at the Horn of Africa, or a plotted terrorist attack of the Ohio trucker Iyman Faris, who planned to bring down Brooklyn Bridge (CNN 2003).

Micro-political risks do not necessarily coincide with aggression and include diplomatic meltdowns, which regularly lead to complete blockades and border closures. As such border closures affect the logistical infrastructures by cutting them, they can be seen as classic examples for micro-political risks. The most striking example for such a complete border closure is the border that separates the Korean Peninsula into the Democratic Republic of Korea and the Republic of Korea. As a result of the impenetrability of the border, the largest logistical infrastructure in history, the proposed 'Asian Highway 1 (AH1)' from Edirne (Turkey) to Tokyo (Japan), has never been passable from its start to its end. Other examples of complete border closure due to diplomatic meltdowns include the Armenian-Turkish land border, which has left the once crucial Kars (Turkey)–Gyumri (Armenia)–Tbilisi (Georgia) railway defunct since 1993 (Uysal 2014). In very rare occasions, even airports can suffer from micro-political risks, when the region the airport is located in is not internationally recognized (anymore). Currently, such theoretically operational, but de facto defunct airports can be found in the disputed territories of Palestine (Watson 2014), Cyprus (Morley 2013), and Nagorno-Karabakh (Asbarez 2016).

Economical risks are usually less relevant for the logistical infrastructure, as the majority of the infrastructure is typically publicly owned and thus well protected against bankruptcy. On the contrary, the few privately owned parts of the logistical infrastructure are often vulnerable to economical risks and can, in some cases, be critical for the overall infrastructures. Most prominently, airports are regularly vulnerable and highly critical simultaneously. The planned 'Berlin Brandenburg Airport', for instance, which should have replaced three smaller airports in Berlin by 2010, but is to date still not operational, caused an average monthly cost of well over 40 million Euro, due to necessary re-routings, re-licensing of the airports to be replaced and other infrastructural follow-up costs. The road infrastructure, which is often completely publicly owned, is also becoming more vulnerable to economic risks whenever public–private partnerships are realized. A warning example for this is the 'Camino Colombia Toll Road', which was built to connect Texas with Mexico, but went bankrupt and was completely closed after only four years of operation (US PIRG Education Fund 2009).

Social risks, by definition, affect individuals or groups of individuals who are then, after the realization of the risk, incapable of retaining their social status. Usually, individuals are not able to debilitate the logistical infrastructure in the following, but again several exceptions prove that social risks can, indirectly, affect logistical infrastructure severely. Most commonly, strikes by workers whose social status is at risk regularly affect the logistical infrastructure. In particular, airports and rail operations are repeatedly brought to a standstill by coordinated strikes. More drastically,

a coordinated general strike directed against the oil supply chain caused a shortage of gas supplies for Greater Paris in 2016. During this orchestrated strike, truckers blocked the road infrastructure leading to and out of the most crucial ports where oil tankers unload the gasoline for the French market (Heusch 2016).

Technological risks for the logistical infrastructure can be further diversified into operational risks, which are directly caused by the usage of the particular infrastructure, and risks concerning the control and maintenance of the logistical infrastructures. A well-known example for an operational risk is the major explosion that hit the Chinese Port of Tianjin in 2016, caused by the handling of explosive goods, which forced the port to be entirely closed for two weeks (DB Schenker China 2015). A recent example for a technological risk caused by insufficient maintenance is the closure of the railway line traversing Germany from North to South in the vicinity of the town of Rastatt, as mentioned above.

Legal risks for critical logistical infrastructures include diplomatic restrictions and blockades as presented in the subsection on micro-political risks above. Furthermore, legal risks can be caused by a temporary or permanent blockade of a single infrastructural part or a whole region for national policy reasons. Finally, unforeseen and sudden changes to the legal framework for logistical operations can severely affect the infrastructure as a whole. A recent example for the latter is the so-called 'refugee crisis' in Europe, which is still ongoing and started approximately in 2015 as a result of the Syrian civil war. When millions of refugees sought shelter in Europe, various European countries, such as Hungary, Austria, Croatia, Serbia, France, and Austria, suddenly closed their borders or at least re-introduced regular border controls, which were formerly unknown within the common Schengen free trade region. Those policy changes, which happened overnight in some cases, led to traffic jams and delays of several days (Turner 2015). Another type of temporary regulatory change is introduced to protect certain events of particular risk. The Chinese city of Hangzhou, for example, was completely off-limits for all logistical transportation during the G20 summit for security reasons (Breakbulk 2016). On a few rare occasions, cities are even permanently cut off from logistical infrastructure by special checkpoints and protected by tightened entry regulations, such as the so-called 'Closed Cities' of Russia.

Ecological risks are risks caused by the natural environment. Such risks are diverse and often have dramatic effects on the logistical infrastructure. Low water levels, floods, earthquakes, typhoons, hurricanes, and other drastic environmental catastrophes regularly debilitate or close down whole road, inland waterway, and rail networks and prevent airplanes from operating. Most dramatically, the Nepali earthquakes of 2015 cut off a large part of Nepalese society from any form of logistical transportation, and thus from all supplies, for weeks (Page 2015). Less drastically, the eruption of the volcano Eyjafjallajökull in 2013 grounded thousands of airplanes across Europe for several days (Randelhoff 2010).

2.1 Categorization and Interdependencies

While the above PESTLE analysis might suggest that risks can be categorized into the described manner, they are in fact often highly interdependent or might fit well into several of the mentioned categories. One extreme example is the risks linked to the Bikini Atoll, which belongs to the Marshall Islands, an independent Pacific Island nation. Political risks, namely World War II and the following Cold War, led to an American interest in the Pacific region and in a national nuclear weapon program, which required a remote testing ground. The US government decided to use the Bikini Atoll as the test ground for its nuclear program, which led to environmental and, as a result of a large re-settlement program, to social risks. Thus, the single event 'nuclear testing in the Bikini Atoll' directly caused three different types of risks, showing how much the different categories can be interwoven. Guyer (2011) describes the whole Bikini Atoll nuclear testing disaster and its consequences in detail.

Similarly, especially as a result of ongoing digitalization, different infrastructures are increasingly interdependent. Today, a power outage has an impact on the IT infrastructure, which again has an impact on both the logistical and the freshwater supply infrastructure. Such indirect impacts of a power outage can thus always debilitate other, dependent, infrastructures, which might lead to secondary environmental and social risks. Rinaldi et al. (2001) summarize how different infrastructures are increasingly dependent on each other.

2.2 Existing Methodology

Only a limited number of publications have so far explicitly considered risks for critical logistical infrastructures. In the following, the few existing political and scientific approaches are summarized.

From a political perspective, risk management for critical infrastructures, in particular for logistical infrastructures, has its roots in the USA and can be divided into three eras. In a first era, the then President Bill Clinton introduced the term 'critical infrastructure' in 1996 formally by establishing the 'Commission on Critical Infrastructure Protection', which was set up to define a framework for risk management for critical infrastructures (see President's Commission on Critical Infrastructure Protection (1997)). Furthermore, the first report of the commission initially raised public awareness of the significance of national infrastructures for the welfare and quality of life for US-American citizens. Other national governments and international organizations did not initially adopt the terminology in that era. The suggestions of the commission and media reports focused on the protection of local infrastructures and the identification of criticalities of single links within the infrastructural networks. The overwhelming majority of the concerned risks in this era were thus environmental, operational, and technological risks.

The 9/11 terrorist attacks against the World Trade Center and the Pentagon started the second era of political interest in critical infrastructures. Disruptively, political actors around the world, led by North American and European policy makers, focused on the protection of national and international critical infrastructures. In this second era, nearly all institutional publications and studies focused on the risk of terrorist attacks, which had previously been largely ignored. Among others, Collier and Lakoff (2008) describe the shift of focus in great detail for the USA. Following the US-American role model, the United Nations (CTITF), the UK (CPNI), the European Union (EPCIP), and other political actors established specialized institutions for the risk management of critical infrastructures. While most of those institutions were originally founded to focus on the risk of terrorist attacks, they nearly all define holistic risk management for critical infrastructures as their institutional goal.

The third era, again, started with the realization of a, so far ignored, risk. In 2007, Estonia was hit significantly by the so-called 'Web War I'—a large-scale and coordinated hacker attack against all IT service of the Baltic country (see The Economist 2010). The ongoing attacks led to a full shutdown of all the Internet-based services in Estonia for a full week. Those services could only be restarted by disconnecting the Estonian Internet infrastructure from the international network for almost a month (Jackson 2013). As an institutional countermeasure to Web War I, NATO defined the 'Policy of Cyber Defense' in April 2008 and, subsequently, established the NATO Cooperative Cyber Defense Centre of Excellence (Herzog 2011). After more cyberattacks against the former Soviet States of Lithuania 2008, Georgia 2008, and Kazakhstan 2009, for all of which Russia was found responsible, the topic of 'cybersecurity' got even more into the focus of NATO. It was finally entirely interwoven with the thematical complex of infrastructure protection at a NATO ministerial conference with the topic 'critical infrastructures and cybersecurity' in April 2009 (Bumgarner and Borg 2009). As result of a perceived decreasing risk of terrorist attacks and an increased risk of cyberattacks from 2007/2008 on, the focus of the institutional work for protecting critical infrastructures subsequently shifted mainly to the protection of information infrastructures.

Recent events, like the activities of the so-called 'Islamic State', shift back the focus on the risks of terrorism and away from cyberthreats (Stock 2017).

The political and institutional eras of risk management for critical infrastructures reflect the 'Western World' view, which was led by the USA, Canada, and Europe. In other parts of the world, the above eras did not happen to the same extent. The People's Republic of China, for instance, still did not formally define the term 'critical infrastructure' or establish an institution that is responsible for protecting it. Other countries focus on risks that are most relevant for them. The British Virgin Islands, for example, focus entirely on environmental risks, like tornados (Penn 2010).

Scientifically, probably the first approach for the protection, or destruction, of a critical infrastructure was published by the US-American think-tank 'RAND Corporation', which mainly conducted contract research for the US Navy in the 1950s. The mathematician T. E. Harris specified, together with former general D. F. S. Ross, the so-called 'Maximum Flow Problem' in 1955 (Harris and Ross 1955), which became a classic optimization problem. That problem is solved to determine the maximal

(one-dimensional) flow of goods within a network. Together with two other RAND Corporation members, L. R. Ford Jr. and D. R. Fulkerson, Harris developed the first efficient and exact procedure to solve this combinatorial problem. Furthermore, he discovered and proved the 'Max-Flow-Min-Cut Theorem', which observes that the maximum flow of a certain network has exactly the same value as the minimum cut of the same network. Since the publication of the work of Harris and Ross in 1999, it became clear how this seemingly theoretical work helped the US Navy in military planning. As a 'case study', Harris and Ross calculated the maximum flow of goods from the Soviet Far East to Eastern Europe through the Soviet railway network. Furthermore, the authors observed that a minimum cut would have the same value and made a proposal to military strategists how to calculate such a minimum cut for any possible network. This observation, linked with a remark within the publication, that 'airstrikes are an effective option to debilitate a railway network to prevent the transportation of troops and military equipment', showed why the US Airforce invested in this first-ever scientific research that identified critical infrastructures (Schrijver 2002).

The early research of the RAND Corporation founded an entire research topic, which is best described as 'search for the most critical edge(s).' As such a criticality measurement is most relevant for military applications, either for directed attacks or for an effective defense, this research field grew steadily during the Cold War (see, i.e., Wollmer 1963, 1964, 1968; Fulkerson and Harding 1977; Lubore et al. 1971; McMasters and Mastin 1970; Ratliff et al. 1975; Corley and Chang 1974; Golden 1977; Corley and Sha 1982; Malik et al. 1989 and Ball et al. 1989).

Shortly after the end of the Cold War, the tone and the applications of the research field changed instantly. Suddenly, the search for the most critical component of a network became a purely theoretical research topic and the problem was subsequently defined as 'Network Interdiction Problem' by Wood (1993).

Within the last decade, as a direct result of the increased political interest in the field, most publications focused on finding the most critical components of critical infrastructures. Brown et al. (2005, 2006) were the first to link both topics. In parallel, Salmerón et al. (2004, 2009) presented several approaches to identify the most critical component of an electric grid network. Church and Scaparra (2006) and Scaparra and Church (2008) used the same theoretical foundation to identify the criticality of single network components for the construction of a new facility.

Finally, Alderson et al. (2011) published the first scientific paper which focuses on identifying the critical infrastructure within a general logistical network.

In addition to those contributions from a rather analytical background, a few papers from a risk management perspective did consider risk management for critical infrastructures in particular. Sapori et al. (2014) proposed a generic analytical risk management methodology to manage risks of a critical infrastructure, while Avritzer et al. (2012) broadly show both the challenges and the limits of a systematic risk management for critical infrastructures.

Adar and Wuchner (2005) published an overview of the current state of risk management for critical infrastructure from a business perspective.

They emphasize the central importance of an extensive risk management for critical infrastructure for the success of any economic and public actor.

It can be observed that almost all of the mentioned scientific works on risk management for critical logistical infrastructures focus on the possible economic losses through a potential risk realization. However, it is important to emphasize that critical logistical infrastructures are not only relevant to businesses but are an integral part of the daily life of most citizens. Thus, a risk management for critical logistical infrastructures always has a large value for a society as a whole. To address such social effects of a debilitated logistical infrastructure, the World Bank established and spearheaded a scientific research branch called 'Social Risk Management', which is extensively described by Holtmann et al. (2001) and Holzmann et al. (2003) and critically questioned by Godfrey et al. (2009).

Finally, two often-cited publications discussing the scientific focus of risk management for critical infrastructures should be mentioned. Cardona (2004) tried to understand risk management for critical infrastructures as a holistic research topic and unite or cooperate between the various research fields, namely risk management, network theory, social sciences, and security sciences. Finally, Boin and McConnell (2007) discuss the limits of a risk management for critical infrastructures and link the field with resilience management, which tries to recover an infrastructure as soon as and as less cost-intensively as possible after a risk is realized.

3 Evaluation of Risks for Critical Logistical Infrastructures

3.1 Basic Assumptions

When we talk about logistical infrastructure, we include all relevant stationary facilities that are required to execute the basic logistical processes (i.e., transportation, handling, and warehousing). The logistical infrastructure contains roads, railways, inland waterways, pipelines, but also warehouses and transshipment points such as ports, airports, container terminals, and others.

The logistical infrastructure can be modeled as a network. The warehouses and transshipment points—or in general: the locations where handling, warehousing, and other logistical activities (often called 'value-adding services') take place—are modeled as vertices. Thus, each vertex $v \in V$ represents a logistical facility. On the other hand, the roads, railroads, inland waterways, and pipelines are modeled as edges. Each edge $e \in E$ represents a connection between two logistical facilities. Consequently, the whole logistical infrastructure is represented by the graph $G = (V, E)$.

We assume that for each vertex $v \in V$ and for each edge $e \in E$ the cost for using the specific vertex or edge is known. Thus, a value $c(v) \geq 0$ exists for every $v \in V$, and a value $c(e) \geq 0$ exists for every $e \in E$. This cost should be given as cost per shipping unit.

Our last assumption is that all shipments for a specified period are known a priori. The related shipment data contains at least the source and the sink, both defined as vertices $v \in V$. The shipment data must also contain information about the number of shipping units, so that the cost for a shipment can be calculated. The exact route for a shipment does not have to be given; we can assume that the route can easily be calculated by using established shortest path algorithms.

3.2 Evaluation Approach

The basic approach for evaluating risks for critical logistical infrastructures is based on one more assumption and an elementary cost comparison:

- We assume that there is an overall decision maker (e.g., a policy maker in a ministry or in another public authority) who needs to evaluate and prioritize risks for logistical infrastructures. The decision maker would then analyze one infrastructure element after another, evaluating the risks. In the end, all relevant infrastructure elements are evaluated and can be ranked by the implied consequences of risk events. (For simplicity reasons, we will focus on risks for vertices, such as ports and warehouses. However, the risk evaluation procedure can easily be transferred to all elements of the network including the edges.)
- For evaluating the risk for a certain element of the infrastructure, we will compare the total logistical cost for two specific situations. The 'normal' situation will be specified as a situation without any risks being realized. In such a situation, the total logistical cost C^{norm} will be calculated by the sum of the cost for each edge and for each vertex, if all orders are fulfilled. The situation 'under risk' will be specified as a situation, where (due to a risk being realized) a certain element of the logistical infrastructure is not usable, or the capacity is limited. In such a situation, shipments must be redirected using the remaining network. If the 'normal' situation is characterized by cost-optimal routes, the situation under risk will obviously lead to higher total logistical costs C^{risk}.
- The difference between the cost for the 'normal' situation and the situation under risk will be interpreted as the consequence if a risk for a certain vertex is realized: $\Delta C = C^{risk} - C^{norm}$.

3.3 Implementation

For the implementation of the evaluation approach, we will create an additional matrix A_v for each vertex $v \in V$ that should be evaluated. This matrix A_v only stores the information of the set of orders that are relevant for the evaluation process. This contains exactly those shipping orders O_v that use the specific vertex $v \in V$, which should be evaluated: $O_v = \{(v_1, w_1), \ldots, (v_n, w_n)\}$. All other shipping orders are

considered as irrelevant for the evaluation. In the matrix A_v, the source and sink vertex v_i and w_j for each order as well as the shipping quantity $q_{i,j}$ are saved. This leads to the definition of an element $(a_v)_{i,j}$ of the matrix A_v as $(a_v)_{i,j} = \begin{cases} q_{i,j} \text{ if } (v_i, w_j) \in O_v \\ 0 \qquad \text{else} \end{cases}$.

The graph that represents the logistical infrastructure without the vertex (or vertices) that is affected by the risk event is noted as $\widehat{G} := G[V \backslash R] = \left(\widehat{V}, \widehat{E}\right)$ with $\widehat{V} = V \backslash R$ and $\widehat{E} = \{\, e = (v, w) \in E | v, w \in \widehat{V}\}$.

To calculate C^{norm} and C^{risk}, well-established shortest route algorithms can be applied. For each source/sink combination of the additional matrix A_v that uses the affected vertex, thus with $(a_{v^*})_{i,j} > 0$, the cost can be calculated by summing up the cost per used infrastructure element. This will be determined by multiplying the cost per shipping unit with the shipped quantity. For simplicity reasons, we assume that only edges induce cost. (Again, this assumption can easily be omitted.) The total logistics cost for shipping all orders that use the vertex v^* under normal conditions, thus without the risk realization, are calculated by $C^{norm}_{v^*} = \sum_{(i,j):(a_{v^*})_{i,j}>0} C_{i,j}$. The total logistics cost after the risk event affected vertex v^* is then calculated by $C^{\text{risk}}_{v^*} = \sum_{(i,j):(a_{v^*})_{i,j}>0} \widehat{C}_{i,j}$. In this case, the shortest route algorithms use the subgraph $\widehat{G} := G[V \backslash R] = \left(\widehat{V}, \widehat{E}\right)$.

Finally, the consequence of the risk affecting vertex v^* is calculated as the difference between the total cost of the normal situation and the total cost of the situation under risk, as mentioned above: $\Delta C = C^{risk} - C^{norm}$.

3.4 Strengths, Weaknesses, and Extensions

The evaluation approach presented in the previous sections is considered as a first step in developing a framework for risk evaluation of critical infrastructure. It is characterized by specific strengths, but it also shows room for development. In this section, we discuss such strengths and weaknesses and outline options for further progress.

The evaluation approach is meant to prioritize individual infrastructure elements by the quantified consequences implied by a realized risk event. The results reflect a ranking of infrastructure elements at risk and should be interpreted as a relative outcome and not, as might be expected, by their absolute values. With such results, decisions makers—especially in ministries on federal and regional level as well as institutions—receive relevant information and can focus the development of counteractive measures on those elements of the logistical infrastructure where a risk realization would lead to the highest overall consequences. The results thus lead to an efficient allocation of resources for an effective risk management. The approach can, on the other hand, not be used for evaluating a single element on its own by assignment of 'the real' cost of

a risky event, i.e., the absolute value of all costs that are generated by the risk. Thus, the suggested evaluation approach is not intended to support decision makers on a local level, such as the manager of a single container terminal.

There is a second reason why the approach does not support managers on the element level, but policy makers on higher levels: A risk affecting an element of the infrastructure will lead to negative consequences, i.e., to additional cost, for the analyzed element. If shipments are redirected, they use other elements of the infrastructure. If the providers of the then used infrastructure can create additional revenues, they benefit from a risk that affects other elements. Only a policy maker on a higher level who has responsibility for the overall cost will be interested in the efficient allocation of resources for managing the risks, i.e., for minimizing the total risk-induced costs.

A necessary requirement for comparing risks for elements of the critical logistical infrastructure in the described way is that the risky events are specified identically. For example, a risk event for container terminals could be specified as a 24-hour interruption of all activities due to a breakdown of the power supply. To have a consistent risk evaluation and ranking, all considered terminals should be evaluated for a risk event with the same specification.

Another strength of the approach lies in its simplicity. For evaluating an element of the infrastructure, only the data of the infrastructure network and of those orders that use the specific element is required. This has two positive effects: On the one hand, data collection is relatively easy. If we assume that the cost of data retrieval depends on the amount of data that is necessary, also the cost of data provision is low. On the other hand, the calculation can be done in a short time. The computation time depends on the problem type and on the number of orders for which optimal routes must be calculated. Shortest path problems can be solved in polynomial time, so that the problem type does not lead to unacceptable computation time. By only considering those shipments that explicitly use the selected infrastructure element, the computation time is further reduced.

The simplicity of the approach leads, however, to weaknesses by excluding realistic assumptions. So far, the definition of risk event does not consider a recovery phase, where the capacity of the logistical infrastructure is continuously (maybe stepwise) increased over time, until the normal capacity is reached. Such dynamic processes could be implemented by either dividing the recovery time into discrete elements with increasing capacities and calculating the induced cost for each of the time frames or by applying a simulation approach. Also, the approach does not take into account possible buffers of whole shipments or shipping units in nodes of the logistical networks: As long as the storage capacity of a warehouse or any transshipment point allows for a temporary buffering, this option could be used to avoid re-routing a shipment.

Another weakness of the current implementation is the sole focus on transportation processes (including the implicit use of handling processes) without taking into account value-added services. The model can, however, easily be extended by modeling the possible or required logistical process for each element of the infrastructure.

The last weakness also results from the simplicity of the approach: In the current implementation, we assume that all shipments that use a certain infrastructure element can be re-routed without limitations. That is, the remaining infrastructure network provides enough capacity for all redirected shipments. This might not be the situation in reality: Due to absorbing redirected orders, the capacity of the then used infrastructure might reach its upper limit. This situation can be implemented by defining upper limits for the infrastructure network; the upper limits can take into account some average utilization to include an initial capacity usage. To include possible priorities of shipments, the approach can be extended by using not only the shipments that use the infrastructure element in focus, but all shipments. This way, penalty costs can be used to find an overall optimum, i.e., the cost-optimal routing of all orders minimizing total logistics cost including penalties.

The approach focuses only on the consequences of risky events but does not include the probabilities of those events. This is consistent, since the aim of the approach is to generate a ranking based on the consequences for certain events. Since the calculation for one single risk event and for one specific element of the infrastructure leads to a single result (the cost as the consequence of the risk event), the probabilities (if they can be assessed or estimated) can be used without problems, so that the usual risk parameters (consequence and probability) are considered for decision making.

A last aspect focuses on data availability. The assumption that shipping data is available (especially specifying source, sink, and shipping quantity) does hold for some elements of the infrastructure—but not for all. Usually, ASNs (advanced shipping notices) are sent in electronic form to the partners in a logistics chain, so that such shipping data with the listed data items is available not only for transportation companies, but also for container terminals and other transshipment points, i.e., for the vertices of the network. It is also true for edges of the railway network, because the traffic on the railway network is managed by an institution. On the other hand, the assumption does not hold for infrastructure elements, which do not have to be booked in advance, such as most road infrastructure. For those elements, traffic distribution models for cargo shipments can be used to derive the data, which might not be exact, but offers a reasonable precision for risk evaluation.

4 Summary and Outlook

A structured risk management for critical logistical infrastructures is becoming increasingly important for the most and the least developed countries in the world alike. The most developed logistical infrastructures, like the European road and rail networks, are starting to suffer increasingly from dilapidated and crumbling infrastructural assets, which increasingly require strategically planned maintenance prioritization. On the other hand, developing countries, like those in the Global South, are extending their own road and rail infrastructures rapidly, building thousands of road and rail kilometers every year, and thus have a strong need to strategically distribute

funds to those regions that are currently most vulnerable to being completely cut off by the realization of any potential risk.

The approach presented in the previous section is an easy to implement way for how the risk evaluation phase can be carried out. It supports policy makers on regional and federal levels by creating relevant information on the risk-based ranking of elements of the critical logistical infrastructure. With the evaluation results, such policy makers can create an efficient allocation of resources so that risk management is effective.

Due to its simplicity, the approach has some inherent weaknesses. However, most of the weaknesses can be overcome by extending the model. This can be done by using more data, but also by implementing simulation modules that allow dynamic effects to be considered.

However, it should be noted that the current level of risk management for logistical infrastructure is on a relatively low level: Institutional, regular, and methodologically sound risk management is seldom carried out; thus, the maturity level of risk management is low. On the other hand, data to analyze risks in detail is often not available at all or only on an aggregate level that does not allow for a detailed analysis and evaluation of risk. Therefore, the suggested approach can lead to a large step forward in risk management for critical logistical infrastructure.

References

Abarez (2016). Artsakh determined to open Stepenakert airport for 'people's right to free movement, http://asbarez.com/141373/artsakh-determined-to-open-stepanakert-airport-for-peoples-right-to-free-movement/.

Adar, E., & Wuchner, A. (2005). Risk management for critical infrastructure protection (CIP) challenges, best practices & tools. In *First IEEE International Workshop on Critical Infrastructure Protection*.

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Wood, R. K. (2011). Solving defender-attacker-defender models for infrastructure defense. In K. Wood & R. Dell (Eds.), *Operations research, computing and homeland defense* (pp. 28–49). Hannover, MD: Institute for Operations Research and the Management Sciences.

Avritzer, A., Di Giandomenico, F., Remke, A., & Riedl, M. (2012). Assessing dependability and resilience in critical infrastructures: challenges and opportunities. In K. Walter, A. Avritzer, M. Vieira & A. V. Moorsel (Eds.), *Resilience assessment and evaluation of computing systems* (pp. 41–63). Berlin, Heidelberg: Springer.

Ball, M. O., Golden, B. L., & Vohra, R. V. (1989). Finding the Most vital arcs in a network. *Operations Research Letters, 8*(2), 73–76.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50–59.

Breakbulk (2016). G20 Summit impacts Hangzhou logistics. http://www.breakbulk.com/g20-summit-impacts-hangzhou-logistics/.

Brown, G. G., Carlyle, W. M., Salmeron, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In H. Greenberg & J. Smith (Eds.), *INFORMS tutorials in operations research* (pp. 102–123). Hannover, MD: Institute for Operations Research and the Management Sciences.

Brown, G. G., Carlyle, W. M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530–544.

Bumgarner, J., & Borg, S. (2009). *Overview by the US-CCU of the Cyber campaign against Georgia in August of 2008*. US-CCU Special Report.

Cardona, O. D. (2004). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: A necessary review and criticism for effective risk management. In G. Bankoff, G. Frerks, & D. Hilhorst (Eds.), *Mapping vulnerability: Disasters, development and people* (p. 17). London: Earthscan.

Church, R. L., & Scaparra, M. P. (2006). Protecting critical assets: The r-interdiction median problem with fortification. *Geographical Analysis., 39*(2), 129–146.

CNN (2003). *Ohio trucker joined al Qaeda Jihad*. http://edition.cnn.com/2003/LAW/06/19/alqaeda.plea/.

Collier, S., & Lakoff, A. (2008). The vulnerability of vital systems: How 'critical infrastructure' became a security problem. In: M. Dunn & K. Soby (Eds.), *Securing the homeland: Critical infrastructure, risk and security* (pp. 40–62). London: Routledge.

Corley, H. W., & Chang, H. (1974). Finding the n most vital nodes in a flow network. *Management Science, 21*(3), 362–364.

Corley, H. W., & Sha, D. Y. (1982). Most vital links and nodes in weighted networks. *Operations Research Letters, 1*(4), 157–160.

DB Schenker China (2015). *Explosions in industrial area in Tianjin impacts port operations*. http://www.dbschenker.com.cn/log-cn-en/news_media/news/9842348/explosion_in_tianjin.html.

Fulkerson, D. R., & Harding, G. C. (1977). Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming, 13*(1), 116–118.

Godfrey, P. C., Merrill, C. B., & Hansen, J. M. (2009). The relationship between corporate social responsibility and shareholder value: An empirical test of the risk management hypothesis. *Strategic Management Journal, 30*(4), 425–445.

Golden, B. (1977). A problem in network interdiction. *Naval Research Logistics Quarterly, 25*(4), 711–713.

Guyer, R. L. (2011). Radioactivity and rights—clashes at bikini atoll. *American Journal of Public Health, 91*(9), 1371–1376.

Harris, T. E., & Ross, F. S. (1955). *Fundamentals of a method for evaluating rail net capacities* (No. RM-1573). Santa Monica, USA: RAND CORP.

Heinrici, T. (2017). Rheintalbahn ab 2. Oktober wieder frei. https://www.dvz.de/rubriken/land/schiene/single-view/nachricht/rheintalbahn-ab-2-oktober-wieder-frei.html.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2).

Heusch, P. (2016). Streik und Straßenblockaden legen Teile des Landes lahm. http://www.swp.de/ulm/nachrichten/politik/streik-und-strassenblockaden-legen-teile-des-landes-lahm-13020619.html.

Holzmann, R., & Jørgensen, S. (2001). Social risk management: A new conceptual framework for social protection, and beyond. *International Tax and Public Finance., 8*(4), 529–556.

Holzmann, R., Sherburne-Benz, L., & Tesliuc, E. (2003). *Social risk management: The World Bank's approach to social protection in a globalizing world*. Washington DC, USA: World Bank.

Jackson, C. M. (2013). Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success. *New Voices in Public Policy*, *7*(1).

Lubore, S. H., Ratliff, H. D., & Sicilia, G. T. (1971). Determining the most vital link in a flow network. *Naval Research Logistics Quarterly, 18*(4), 497–502.

Malik, K., Mittal, A. K., & Gupta, S. K. (1989). The k most vital arcs in the shortest path problem. *Operations Research Letters, 8*(4), 223–227.

McKenzie, S. (2016). *Brussels travel: Flights suspended, transit limited*. http://edition.cnn.com/2016/03/22/europe/brussels-explosions-transport-flights-metro-suspended/.

McMasters, A. W., & Mastin, T. M. (1970). Optimal interdiction of a supply network. *Naval Research Logistics Quarterly, 17*(3), 261–268.

Morley, N. (2013). *Bold plan to regenerate derelict Nicosia airport*. http://cyprus-mail.com/2013/09/22/bold-plan-to-regenerate-derelict-nicosia-airport/.
Page, P. (2015). *Nepal earthquake response challenges logistics experts*. http://www.wsj.com/articles/nepal-earthquake-response-challenges-logistics-experts-1430343036.
Penn, A. B. (2010). *The Virgin Islands climate change green paper.* Conservation and Fisheries Department and Ministry of Natural Resources and Labour.
President's Commission on Critical Infrastructure Protection (1997). Critical Foundations—Protecting America's Infrastructures. https://fas.org/sgp/library/pccip.pdf.
Randelhoff, M. (2010). Eyjafjallajökull—Die Auswirkungen in Europa und der ganzen Welt. http://www.zukunft-mobilitaet.net/849/analyse/eyjafjallajoekull-fazit-schaden-flugverkehr-global/.
Ratliff, D. H., Sicilia, G. T., & Lubore, S. H. (1975). Finding the n most vital links in flow networks. *Management Science, 21*(5), 531–539.
Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11–25.
Salmerón, J., Wood, K., & Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Transactions on Power Systems, 19*(2), 905–912.
Salmerón, J., Wood, K., & Baldick, R. (2009). Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems, 24*(1), 96–104.
Sapori, E., Sciutto, M., & Sciutto, G. (2014). A quantitative approach to risk management in critical infrastructures. *Transportation Research Procedia, 3,* 740–749.
Scaparra, M. P., & Church, R. L. (2008). A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research, 35*(6), 1905–1923.
Schlesiger, C. (2017). 75 Millionen Euro Umsatzverlust wegen Rastatt-Sperrung. http://www.wiwo.de/unternehmen/dienstleister/deutsche-bahn-75-millionen-euro-umsatzverlust-wegen-rastatt-sperrung/20477114.html.
Schrijver, A. (2002). *Combinatorial optimization: Polyhedra and efficiency* (24th ed.) (pp. 166–169). Heidelberg: Springer Science & Business Media.
Sottilotta, C. E. (2013). *Political risk: Concepts, definitions*. Challenge. Working Paper Series. LUISS School of Government.
Stock, J. (2017). United Nations Security Council open debate on the protection of critical infrastructure against terrorist attacks. *Statement by Interpol*. https://www.interpol.int/content/download/34261/450506/version/1/file/Statement%20by%20Secretary%20General%20to%20the%20UNSC.pdf.
Turner, C. (2015). *Eurotunnel warns of lengthy delays due to 'migrant activity'*. http://www.telegraph.co.uk/news/uknews/11762469/Eurotunnel-suspends-passenger-services-because-of-migrant-activity-in-Calais.html.
Ukraine Today (2015). *Cyborgs vs. Kremlin*. http://cyborgs.uatoday.tv/.
US PIRG Education Fund (2009). *Private roads, public costs*. http://www.uspirg.org/sites/pirg/files/reports/Private-Roads-Public-Costs-Updated_1.pdf.
Uysal, O. (2014). *10 things to know about baku-Tbilisi-Kars Railway Project*. https://railturkey.org/2014/10/20/baku-tblisi-kars-railway/.
Watson, L. (2014). *Inside the ruins of Gaza's airport*. http://www.dailymail.co.uk/news/article-2730465/Inside-ruins-Gaza-s-airport-Photographs-transport-hub-named-honour-Yasser-Arafat-open-just-three-years-destroyed-neglect-war.html.
Wollmer, R. D. (1963). *Some methods for determining the most vital link in a railway network*. RAND Memorandum, RM-3321-ISA.
Wollmer, R. D. (1964). Removing arcs from a network. *Operations Research, 12*(6), 934–940.
Wollmer, R. D. (1968). Stochastic sensitivity analysis of maximum flow and shortest route networks. *Management Science, 14*(9), 551–564.
Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling, 17*(2), 1–18.
Zaman, A. (2016). U.S. air strikes destroy last Euphrates bridges in Deir Ez Zor. https://en.zamanalwsl.net/news/18649.html.