

Lars Schnieder

PROTECTION OF CRITICAL TRANSPORT INFRASTRUCTURE

A holistic approach

Note: This work was originally published in German: *Schutz Kritischer Infrastrukturen im Verkehr* by Lars Schnieder; Copyright © Springer Fachmedien Wiesbaden GmbH, part of Springer Nature 2018. All rights reserved.

Bibliographic information published by the Deutsche Nationalbibliothek:

The German National Library catalogues this publication in the German National Bibliography; detailed bibliographic information can be found on <http://dnb.de>

Publishing House: PMC Media House GmbH
Werkstättenstraße 18
D-51379 Leverkusen

Office Hamburg: Frankenstraße 29
D-20097 Hamburg
Phone: +49 (0) 40 228679 506
Fax: +49 (0) 40 228679 503
Web: www.pmcmedia.com; E-Mail: office@pmcmedia.com

Managing Directors: Detlev K. Suchanek, Antonio Intini
Editorial Office: Dr. Bettina Guiot
Proofreading: John Glover
Distribution/Book Service: Sabine Braun
Advertisements: Dirk Bogisch

Cover Design: Pierpaolo Cuzzo (TZ-Verlag & Print GmbH, Roßdorf)
Typesetting and Printing: TZ-Verlag & Print GmbH, Roßdorf

© 2019 PMC Media House GmbH, Hamburg
1st edition 2019

ISBN 978-3-96245-168-4

This publication and all its parts are protected by copyright. Any exploitation beyond the restricted use of copyright law and without the publisher's consent is prohibited and unlawful. This applies in particular to any form of reproduction, translation, microfilming and incorporation and processing in electronic systems.

A publication by


PMC Media
International Publishing

What you can find in this ABSTRACT

- A definition of critical transport infrastructure
- A motivation to protect critical transport infrastructure based on the legal framework
- An overview of the institutional framework to ensure the security of critical transport infrastructure within the European Union
- Derivation of the appropriate and proportionate level of protection for critical transport infrastructure
- Defence in depth as a holistic approach for the protection of critical transport infrastructure

Summary

Transport infrastructure plays a vital role in our society. Deliberate harmful actions intended to damage or interrupt the use and operation of transport infrastructure can affect negatively the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy.

This book addresses the question of what is meant by critical transport infrastructure. Network and information systems are essential for its effective control. That is why these systems in particular need to be protected against unauthorised access. The motivation of companies and organisations to secure the critical transport infrastructure which they operate is based on a uniform legal framework imposed within the European Union.

EU legislation has to be transformed into national laws by each one of the member states. It is the ultimate goal of legislation at European level to set out an equal level of protection of consumers and businesses to cybersecurity threats. In order to do so, operators of critical transport infrastructure first of all need to be identified. These operators then need to define the requirements for protection measures, in proportion to the risks represented to their networks. Such risks need to take into account the current state of the art of cybersecurity.

Following the design paradigm of defence in depth, an effective protection of critical transport infrastructure can only be achieved with an adequate combination of technical and organisational measures, as well as the appropriate physical protection of the relevant assets.

Foreword

A life without a smartphone and a tablet is hardly conceivable for many of us. “Always on” – unrestricted connectivity is now one of the basic needs of our society. There is hardly any area in our daily life that does not depend on some kind of digital infrastructure and network and information systems. This applies equally to urban, national and international transport infrastructure.

The rapid pace of innovation and technological development regularly brings forward new threat scenarios for network and information systems. In consequence this increases the need to face the challenges of cybersecurity of both the system suppliers as well as operators integrating them into their overall system architectures. It is quite obvious that threats from the internet must at no time manipulate the software in network and information systems supporting traffic control, which is essential for the viability of our society and economy.

The Commission of the European Union has introduced EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. This directive calls for extended requirements for critical transport infrastructure which has to be introduced in all member states. Legislation requires the operators of critical transport infrastructure to take appropriate organisational and technical measures to prevent disruptions to the availability, integrity, authenticity and confidentiality of their network and information systems relevant to the functioning of the critical transport infrastructure they operate.

This book outlines the basis for the security of critical transport infrastructure, along with the corresponding institutional framework. It introduces the criteria based on which critical transport infrastructure is identified and shows how appropriate and proportionate protection of critical transport infrastructure is carried out. This combines technical measures with organisational measures and physical protection.

Braunschweig, Germany

Dr.-Ing. Lars Schnieder

Content

Summary.....	5
Foreword.....	7
1 Legal Framework of Critical Infrastructure.....	11
1.1 Definition of Critical Transport Infrastructure.....	11
1.2 Legal Basis for the Protection of Critical Transport Infrastructure.....	12
1.2.1 Harmonisation of Legal Bases in the European Union	12
1.2.2 Statute Law as a Basis	13
1.2.3 Specification by Regulatory Law	14
1.2.4 Standards as a Measure of What Is Legally Required	14
2 Liability Avoidance as Motivation for the Protection of Critical Transport Infrastructure	17
2.1 Liability in Corporate Law	19
2.2 Liability in Public Law	19
2.3 Liability in Civil Law	20
2.4 Liability in Criminal Law.....	21
3 Quality Assurance Chain for the Protection of Critical Transport Infrastructure	23
3.1 Product Regulation.....	23
3.2 Accreditation.....	24
3.3 Conformity Assessment and Certification.....	25
3.4 Approval	25
3.5 Product Surveillance	26
3.6 Market Surveillance	27
4 Defence in Depth – Holistic Approach for the Protection of Critical Transport Infrastructure.....	29
4.1 Protection by Hardening Information Technology Systems	29
4.1.1 Threat Analysis and Risk Assessment (TARA).....	29

4.1.2	Derivation of Security Requirements	30
4.1.3	Verification and Test of Security Requirements	32
4.2	Protection by Physical Measures	34
4.2.1	Prevention of Unauthorised Access.....	35
4.2.2	Detection of Unauthorised Access	36
4.2.3	Intervention in Case of Unauthorised Access	36
4.3	Protection by Organisational Measures	37
4.3.1	Characteristics of Information Security Management Systems (ISMS)	37
4.3.2	Continuous Improvement (PDCA cycle).....	37
5	Conclusions and Outlook.....	39
	References.....	41
	Abbreviations.....	43
	Index	44
	The Author	46

1 Legal Framework of Critical Infrastructure

Network and information systems play a vital role in our society. Their integrity and availability are essential to economic and societal activities. Transport infrastructure especially plays an important role in facilitating the cross-border movement of goods, services and people. Due to the importance of such infrastructure, a comprehensive legal framework has been established to protect it against deliberate harmful attacks intended to damage or interrupt their operation. This introductory chapter defines the concept of critical transport infrastructure and sets out the relevant European legal basis from which national law is derived.

1.1 Definition of Critical Transport Infrastructure

The supply of our society with services such as energy, drinking water, health care, financial services and banking, as well as transport, is essential. The failure or impairment of these services would result in significant supply shortages or threats to public safety. Therefore, these services are also referred to as *essential services* (see figure 1). Critical infrastructure includes facilities required to provide these *essential services*. Figure 1 provides an overview which sectors of our economy are considered to provide essential services.

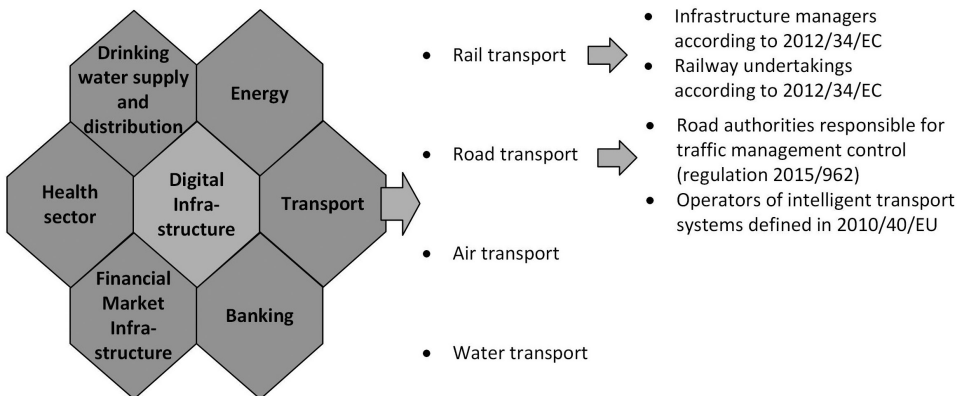


Figure 1: Sectors considered as operators of essential services

Critical Infrastructure. Critical Infrastructure (CRITIS) consists of organisations or institutions of major importance to the society, the failure or impairment of which would result in a sustained supply shortage, significant public security disruption, or other dramatic social consequences. For this reason critical infrastructure security (CRITIS) is a high priority within the European Union

A functioning and efficient transport system is a basic requirement for a modern economy. Given the extensive division of labour, unhindered mobility of goods and persons is of utmost importance. Furthermore, the globalisation of production and sales of goods as well as the development of international passenger traffic have experienced rapid growth in recent years. As a result the

transport infrastructure has become a key factor in supplying the economy as well as our society with goods and services. This importance can be deduced directly from transport statistics. More than 4.1 billion tonnes of goods and more than 70 billion people were transported in the year 2014. In addition, special attention needs to be paid to the fact that the transport sector is highly interrelated to other sectors. Disturbances in one sector are likely to spread to the others.

This interdependency can be explained with the following example:

- *Disruptions or breakdowns in the transport infrastructure* affects almost all other areas of society and economic life. Within a short period of time, the economy is greatly affected by delays in the production and delivery of goods as well as the availability of personnel. Likewise, prolonged disruptions also sustainably affect the administration and social life. The consequences of such disruption would be an inadequate supply of essential goods, a negative impact on rescue and health care and, among other things, a lack of mobility for work and leisure.
- *Disruptions and failures in other sectors* in turn affect the transport sector. An example is the provision of the energy needed to carry people and goods. In addition, driven by the increasing digitisation of transport, network and information systems have become increasingly important. Their failure can make the provision of transport services very difficult.

The transport and transport sector comprise passenger and freight transport by road, rail, air, inland and maritime transport, as well as the logistics sector. In this book, the focus is on land-based transport modes.

1.2 Legal Basis for the Protection of Critical Transport Infrastructure

Legal norms are in a hierarchical relationship with one another (see figure 2). Moreover, as shown in figure 2, the national legal system is integrated into the legal framework of the European Union. This section outlines the individual elements of the regulatory framework for security of networks and information systems used for traffic control.

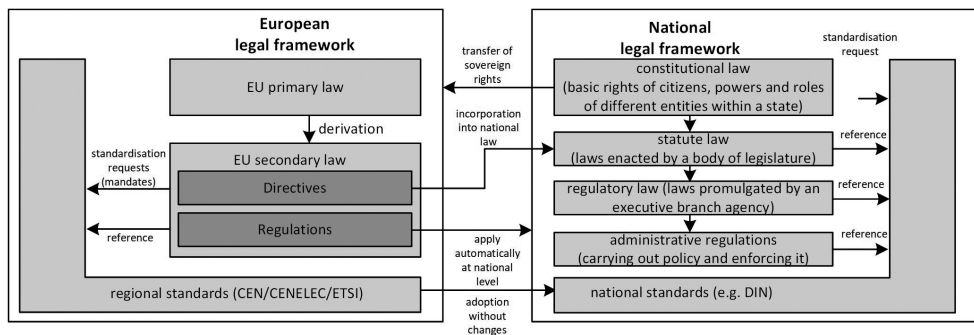


Figure 2: Embedding of national legal acts in the European legal framework (Schnieder 2017a)

1.2.1 Harmonisation of Legal Bases in the European Union

Harmonisation refers to the mutual harmonisation of national laws and regulations of the member states on the basis of European legislation. European law can be differentiated in the following way (left side of figure 2):