Editorial

Khalid Bichou*

Port Operations, Research and Technology Centre (PORTeC),
Centre for Transport Studies,
Imperial College London,
Skempton Building, SW7 2BU, UK
E-mail: Khalid.bichou04@imperial.ac.uk
E-mail: khalidbichou@googlemail.com
*Corresponding author

Michael G.H. Bell

Institute of Transport and Logistics Studies (ITLS),
University of Sydney,
173-175 Phillip Street,
Sydney, NSW 2000 C13, Australia
E-mail: michael.bell@sydney.edu.nk

Biographical notes: Khalid Bichou is a port and transport logistics consultant with over 23 years of experience including periods in senior positions and as consultant and advisor to public and private bodies. Parallel to his professional career, he has a strong interest in academic research and teaching. He has published five books (including *Port Operations Planning and Logistics*) and over 80 academic papers. He is a Co-Founder of PORTeC at Imperial College London where he is a Visiting Reader. He is a Senior Visiting Fellow of Maritime Operations and Management at City University London, and holds visiting research and teaching positions at other universities.

Michael Bell is the Foundation Professor of Ports and Maritime Logistics in the Institute of Transport and Logistics. Prior to his commencement at the University of Sydney in August 2012, he was a Professor of Transport Operations and Director of the Port Operations Research and Technology Centre (PORTeC) at Imperial College London. He is the author of many papers, a number of books (including *Transportation Network Analysis*, published in 2007) and was for 17 years an Associate Editor of *Transportation Research B*.

Supply chain security is often associated with the robustness and/or vulnerability to supply chain failures and disruptions. Global supply chain networks have been designed to respond to market and operational requirements, but their robustness and reliability with respect to random or targeted failures has been questioned. Potential sources of disruption to supply chains are numerous, ranging from routine events like strikes, process and system failures to natural disasters like earthquakes, hurricanes, floods, volcano eruptions, and large epidemics. In the post-9/11 era, the focus has shifted to events involving malevolence such as terrorism, piracy, counterfeiting, theft, smuggling and illegal trafficking.

Ensuring the robustness and stability of supply chains is a high priority. Businesses and governments alike have taken steps towards protecting supply chains by reducing the exposure to hazards and the impacts of disruptions. Researchers have also addressed various aspects of supply chain security including threats, risks, resilience, mitigation and recovery. Nonetheless, the global scope and wider impacts of supply chain insecurity remain under-researched and fragmented. On the one hand, there is a need to integrate and manage the different aspects and components of supply chain security. On the other, there is a need to address industry- and firm-level impacts of supply chain disruptions.

The main objective of this special issue is to shed light on the recent developments in the field of supply chain security focusing in particular on the security of transport and intermodal supply chains. Seven original papers, drawn from 18 submissions, have been selected for this special issue. The selected papers are all empirical and use a mix of quantitative and qualitative frameworks to identify and assess the risks and impacts of supply chain security in the context of intermodal and transport operations. Some papers go further by proposing and testing solutions for protecting intermodal supply chains and enhancing their resilience and robustness in the event of failures and disruptions.

The first paper by Männistö, Hinsta, and Urciuoli attempts to categorise and analyse supply chain crime based on a perception survey about crime threats and problems to commercial supply chains. The result is a supply chain crime taxonomy that categorises crime problems into six classes namely: theft and robbery, trafficking, damage from the inside, damage from the outside, violation of the rules of legitimate commerce, and crime facilitation. The developed taxonomy is further validated in a case study of a Swiss postal operator.

The second paper by Pero and Sudy reports on a qualitative framework designed for improving the security of containerised supply chains, as part of the IMprove the supply chain for COntainer transport and integrated SECurity (IMCOSEC) simultaneously project. Following an extensive literature review, the authors developed a five step supply chain security approach ranging from the identification and assessment of supply chain threats to the implementation and performance monitoring of identified target processes. The proposed approach was then applied and tested through several interviews and expert workshops.

The third paper by Boile and Sdoukopoulos investigates the relationship between supply chain visibility and security and the role of technology in improving them. Focusing on containerised and intermodal supply chains, the authors conducted several stakeholder interviews and a dedicated workshop to identify the critical requirements for the industry's supply chain needs. A technological platform was then developed to provide real-time information on the containers' location and integrity, and was evaluated following an extended large-scale demonstration as part of the SMART container management (SMART-CM) project.

The fourth paper by Doll, Papanikolaou, and Maurer examines the vulnerability of European transport networks to extreme weather conditions. The authors used economic assessment accounting-based methods to estimate the costs of disruptions to transport infrastructure assets stemming from various scenarios of extreme weather conditions. Their estimation is that the average impact of selected weather categories on the EU transport network would cost an average of €2.5 billion annually. The authors then used a network efficiency model to assess the criticality of transport networks in the case of the Greek road transport network.

The fifth paper by Talas and Menachof looks at the relationship between residual security risk and security investment in the context of port security, most notably ISPS Code compliant port facilities. Based on survey data about three main security systems across six port facilities, the authors calculated the security costs, the residual risks and their cost-benefit ratios. They then used portfolio optimisation to examine and select among 216 possible portfolio combinations the portfolios that provide the greatest reduction in security investment and residual security risk.

The sixth paper by Trepte and Rice explores the issue of port capacity and resilience in the USA. Based on a combination of a statistical analysis of documented US port failures and a capacity dispersion commodity model in the event of a disruption at a major US port, the authors concluded that there is not enough capacity at the various major ports to handle a catastrophic disruption without a significant impact on the US economy.

The last paper by Jażdżewska-Gutta investigates supply chain security issues in Poland. The Polish case is somewhat specific in that much of freight transport is undertaken by road and where cargo thefts and attacks on drivers are shown to be the main risks to supply chains. To further examine these issues, the author has carried out a survey among transport and logistics companies in Poland with a view to assessing their perception of supply chain risks, costs and regulatory compliance. The survey findings show that the most reported supply chain risks are debt collection difficulties and cargo thefts and smuggling. Other findings also show how Poland deviates from most EU countries in terms of regulatory compliance with programmes such as the AEO being used as a means to facilitating trade and customs procedures rather than a tool for enhancing supply chain security.