Mitigating Crime Risks in the International Logistics Network: the Case of Swiss Post

THÈSE N^{O} 6513 (2015)

PRÉSENTÉE LE 29 JANVIER 2015

AU COLLÈGE DU MANAGEMENT DE LA TECHNOLOGIE
CHAIRE LA POSTE EN MANAGEMENT DES INDUSTRIES DE RÉSEAU
PROGRAMME DOCTORAL EN MANAGEMENT DE LA TECHNOLOGIE

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Toni Antero MÄNNISTÖ

acceptée sur proposition du jury:

Prof. D. Foray, président du jury
Prof. M. Finger, directeur de thèse
Prof. A.-P. Hameri, rapporteur
J. Hintsa, rapporteur
Prof. Ph. Wieser, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE
Suisse
2015

Abstract

The terrorist attacks of September 11, 2001 raised major concerns about the vulnerability of global transportation systems to transnational crime and terrorism. Although the attacks occurred in the context of passenger transport, they spurred unprecedented academic research on supply chain security (SCS). Alas, today, more than a decade later, theoretical underpinnings of the SCS discipline remain weak. First, the extant SCS literature offers only a cursory and ambiguous view on the risks that SCS management addresses. Second, the academic research offers little evidence of how security solutions affect security and logistics performance. Due to the scarce and conflicting scientific evidence, managers and authorities are having a difficult time securing the supply chain without disrupting trade and logistics operations.

This thesis comprises three research phases that seek to address the two crucial weaknesses of the current academic knowledge. The first phase intends to identify and characterize risks that the SCS management addresses and capture them under a unified theoretical frame – a taxonomy of supply chain crimes. The taxonomy results from a study of managerial descriptions of crime problems that occur or could occur in the supply chain context. The second phase aims at producing a research agenda and at isolating principles for logistics-friendly design of security systems through a synthesis of peer-reviewed academic SCS literature. The synthesis is done using the so-called systematic literature review technique, which follows a prescribed and transparent protocol devised to reduce researcher bias and increase transparency of the review process. The third research phase describes the international postal service from the perspective of Swiss Post, putting a special emphasis on postal security management and law enforcement. The later case study analysis tests validity of the supply chain crime taxonomy and aims to generate evidence-based concepts for improving the postal security management.

Research findings imply that supply chain crime problems are numerous and diverse, most important being cargo theft, smuggling, and cyber crime. Despite the variety, however, the crime problems collapse into three main taxonomic classes when categorized by the way criminals interact with the supply chain: 1) by taking assets out of the supply chain, 2) by introducing unauthorized goods into the supply chain, and 3) by directly attacking the supply chain. Besides, the criminals commonly resort to a range of facilitating crimes to carry out crimes of the main taxonomic classes. The literature

synthesis found that the SCS discipline has attracted cross-disciplinary and steadily growing academic interest over the past decade. The synthesis also suggested that although there are no universal optimal rules for the SCS management, there are certain design principles that should be considered when SCS management decisions are made. The case study evidence revealed that postal security management comprises multiple domains, each having distinctive goals and employing different security solutions. Except for the airmail domain, the number and stringency of existing postal security controls seem low, though proportional to the current terrorist and crime threats. Application of the design principles into the case study context identified a set of promising concepts for improving the postal security management. In particular, future postal security management should focus on compliance monitoring of existing regulations (rather than introducing new rules), security-oriented human resource management, building of capabilities to cope with security-induced uncertainty, and sharing of security control evidence and intelligence.

Keywords: Supply chain security, supply chain risk management, postal service, supply chain crime, contraband, cargo theft, terrorism, trade facilitation, border controls

Abstract

Gli attacchi terroristici dell'11 settembre 2001 hanno sollevato preoccupazioni riguardo la vulnerabilità dei sistemi di trasporto globale a crimini e terrorismo multinazionali. Nonostante gli attacchi abbiano avuto luogo nell'ambito del trasporto di passeggeri, essi hanno dato origine ad un vasto filone di ricerca accademica focalizzato sulla sicurezza della Supply Chain (SSC). Malgrado i progressi della ricerca accademica in questo ambito, ancora oggi, a distanza di più di una decade, il contributo teorico della letteratura rimane ancora debole. La letteratura esistente offre, innanzitutto, una visione sbrigativa e ambigua sui rischi che la gestione della SSC gestisce; inoltre, le evidenze riguardo le modalità con cui le soluzioni per garantire la sicurezza influenzano le performance della sicurezza e della logistica sono ridotte. A causa di queste scarse e contrastanti evidenze, manager e autorità hanno difficoltà nel garantire la sicurezza della Supply Chain senza perturbare l'operatività commerciale e logistica.

La presente tesi include tre fasi che cercano di dare una risposta a questi due punti ancora deboli nell'attuale ricerca accademica. La prima fase vuole identificare e caratterizzare i rischi che la gestione della SSC affronta e classificarli all'interno di un *framework* teorico – una tassonomia dei crimini della Supply Chain. Questa tassonomia è il risultato dell'analisi dei resoconti manageriali sui problemi legati al crimine che hanno luogo ad oggi o potrebbero aver luogo lungo la Supply Chain. La seconda fase vuole creare, attraverso una sintesi della letteratura *peer-reviewed* riguardante la SSC, un'agenda di ricerca e isolare i principi per la progettazione di sistemi di sicurezza che non perturbino la logistica. Questa sintesi è stata condotta attraverso una sistematica revisione della letteratura che ha seguito un protocollo sistematico e trasparente. La terza fase della ricerca descrive, invece, il servizio postale internazionale di Swiss Post focalizzandosi in particolare sulla gestione della sicurezza postale e gli adempimenti legislativi. Questo caso studio esamina la validità della tassonomia dei crimini nella Supply Chain sviluppata e intende sviluppare suggerimenti basati sulle evidenze provenienti dal caso per migliorare la gestione della sicurezza postale.

I risultati della ricerca suggeriscono che i problemi legati al crimine nella Supply Chain sono numerosi, e i più importanti sono furti della merce, contrabbando e cyber-crimini. Nonostante questa varietà, caratterizzando i crimini in base alle modalità di interazione dei criminali con la Supply Chain stessa, essi ricadono all'interno di tre classi tassonomiche: 1) la sottrazione di beni dalla Supply Chain, 2) l'immissione di beni non

autorizzati nella Supply Chain, e 3) l'attacco diretto la Supply Chain. Inoltre, i criminali generalmente ricorrono ad una serie di crimini facilitanti per portare a termine i crimini inclusi nelle classi della tassonomia appena menzionate. Dalla sintesi della letteratura è emerso che la SSC ha attratto stabilmente l'interesse accademico durante la scorsa decade in diverse discipline. Questa sintesi, inoltre, suggerisce che, sebbene non esistano regole ottimali e universali per la gestione della SSC, esistono dei principi di progettazione della Supply Chain che dovrebbero essere considerati in fase decisionale. Le evidenze provenienti dal caso studio rivelano che la gestione della sicurezza postale include diversi ambiti che presentano molteplici obiettivi e diverse soluzioni per la gestione della sicurezza. Eccezion fatta per l'ambito della posta aerea, il numero e la severità dei controlli sembrano essere ridotti, sebben proporzionati alle attuali minacce terroristiche e criminali. L'applicazione dei principi di progettazione della Supply Chain nel caso studio ha permesso l'identificazione di un set di promettenti idee per il miglioramento della gestione della sicurezza postale. In particolare, la gestione della sicurezza postale in futuro dovrebbe focalizzarsi sul monitoraggio della conformità agli ordinamenti esistenti (anziché introdurre nuovi ordinamenti), sulla gestione delle risorse umane in base ad obiettivi di sicurezza, sullo sviluppo di competenze per reagire all'incertezza nella sicurezza, e sulla condivisione di evidenze e *intelligence* riguardanti il controllo della sicurezza.

Parole chiave: sicurezza, gestione del rischio, Supply Chain, servizio postale, crimine, contrabbando, furto di merce, terrorismo, facilitazione del commercio, controlli doganali

Acknowledgements

Writing this doctoral thesis has been a long journey that would have not been possible without help of many people. First of all, I would like to thank my thesis advisor Prof. Matthias Finger for his vital support, advice, and trust during this journey. Thank you for giving me a great degree of freedom to do research on my own terms and for having patience to wait for results. I would also like to express my gratitude to Dr. Juha Hintsa, another key mentor. Thank you for introducing me to supply chain security, for funding the first years of my research, and for providing your invaluable expert advice throughout the years. Besides Prof. Finger and Dr. Hintsa, I would like to thank the three other members of my thesis committee Prof. Ari-Pekka Hameri, Prof. Philippe Wieser, and Prof. Dominique Foray for constructive feedback and insightful questions that helped me to improve quality of my dissertation.

Over the past three and half years, I have had a pleasure of working with many other brilliant people who have helped me to pursue my PhD. I am particularly grateful for support of my previous and present colleagues at the Chair Management of Network Industries (MIR). I would also like to thank personnel at the College of Management who have helped me to navigate through university bureaucracy and overcome technical problems. Furthermore, I would like to express my warm thanks to my fellow PhD students for peer support and for sharing many great moments on- and off-campus. Special thanks go to Ms. Giada Baldessarelli for the Italian translation of the abstract of this dissertation. *Grazie mille!* I would also like to thank my colleagues Dr. Luca Urciuoli and Mr. Juha Ahokas for their expert advice that has helped me to understand better many complexities of our common research field, supply chain security. I would also like to express my gratitude to Dr. Sangeeta Mohanty, Mr. Vladlen Tsikolenko, and other colleagues who have provided me assistance in many ways. I feel grateful for people at Swiss Post for giving me this unique opportunity to study postal security management and build my own expertise on the topic. I would like to present my special thanks to Mr. Fabrizio Simona who made my collaboration with Swiss Post possible by introducing me to right people and by offering his indispensable guidance and expertise. All in all, I would like to send warm regards to all those people who have contributed to my research but whose names I cannot mention here for confidentiality reasons. You know who you are. Thank you!

I am grateful for financial support I have received from Cross-border Research Association and the Chair Management of Network Industries (MIR) throughout my PhD studies. I also greatly appreciate the fact that I have had an opportunity to contribute to and receive funding from SAFEPOST, FOCUS, and CASSANDRA projects that the European Commission has financed under the 7th Framework Programme (grant agreement numbers no. 285104, no. 261633, and no. 261795, respectively). I also appreciate a lesser but anyhow meaningful scholarship that a Finnish foundation Jorma ja Märtha Sihvolan Säätiö has granted me at the beginning of my PhD studies.

Most importantly, I owe a great deal to my girlfriend Gaëlle who has supported and encouraged me through my studies, even on days of frustration and confusion when the PhD seemed only an elusive dream. And last but not least, I would like to thank my family for your unconditional love. *Kiitos.*

Lausanne, January 2015

Toni Männistö

Terms and abbreviations

AEI	Advance Electronic Information
AEO	Authorized Economic Operator
C-TPAT	Customs-Trade Partnership Against Terrorism
CBP	U.S Customs and Border Protection
CBRNe	Chemical, biological, radiological, nuclear, and explosive weapons
CITES	The Convention on International Trade in Endangered Species of Wild Fauna and Flora
CSI	Container Security Initiative
DG MOVE	Directorate General for Mobility and Transport
DG TAXUD	Directorate General for Taxation and Customs Union
DHS	Department of Homeland Security
e-CSD	Electronic cargo security declaration
EC	European Commission
EDI	Electronic Data Interchange
ENS	Entry Summary Declaration
EU	European Union
EXS	Exit Summary Declaration
HRCM	High Risk Cargo and Mail
IATA	International Air Transport Association
ICAO	International Civil Aviation Association
IMO	International Maritime Organization
IPC	International Post Corporation
ISPS code	International Ship and Port Facility Security code

RFID	Radio Frequency Identification
SCRM	Supply chain risk management
SCS	Supply chain security
TAPA	Transported Asset Protection Association
TSA	Transportation Security Administration
UPU	Universal Postal Union
WCO	World Customs Organization

Table of Contents

Chapter 1 | Introduction

This chapter provides an outlook on key debates, regulations, initiatives, and institutional developments that have shaped the research and the practice of the supply chain security (SCS) management since 2001. After the brief introduction, the chapter frames research problems that this doctoral research seeks to address, formulates related research questions, and motivates research from the academic and practical perspectives.

1.1. Background

Few events have had as abrupt and long lasting impact on the international transportation and logistics as the terrorist attacks of September 11th 2001. Although the attacks occurred in the context of passenger transport, they raised concerns about the vulnerability of global supply chains to terrorist attacks and exploitation. Almost overnight, the focus of supply chain security (SCS) management changed from theft prevention to counter-terrorism (Lee and Whang 2005), and the focus of border controls shifted from revenue collection towards border security (Widdowson 2005). Not long after, the paradigm shift translated into an avalanche of government-driven mandatory regulations and voluntary initiatives that aimed to strengthen security across the end-to-end global supply chain, all the way from raw material suppliers to consumers (Sheu et al. 2006; Hintsa et al. 2009). The new security-centric operational environment forced companies to reconsider their approaches to supply chain risk management (Sheffi 2001): How to operate under the heightened threat of international terrorism? How to prepare to cope with consequences of possible new attacks? Ever since the 9/11 tragedy, the SCS management has been a key dimension in a firm's overall supply chain risk management strategy (Williams et al. 2008) and a strategic necessity of doing business (Sarathy 2006).

The importance of the SCS management becomes apparent when considering actual and possible ramifications of criminal and terrorist activities in supply chain context. The logistics networks are capable of moving weapons and tools of terrorism. In the most disturbing scenario, terrorists would dispatch nuclear, radiological, biological, or chemical weapons through the global supply chain to attack their targets from distance. Meade and Molander (2006) estimate that if a nuclear device detonated in a sea container in the port of Long Beach,

California, the blast and the resultant fallout would grind maritime logistics into a halt and induce one trillion USD cost in terms of spending for medical care, insurance claims, workers' compensation, evacuation, and re-construction. Besides the terrorism, the commercial supply chains underpin illegal cross-border trade in narcotics, counterfeits, hazardous waste, untaxed commodities, unlicensed firearms, and stolen goods – virtually any contraband under the sun. The illicit traffic, which is estimated to account for 7 to 10 % of the value of the world trade (WEF 2012), exacerbates many global problems, including arms proliferation, drug abuse, and degrading environment. What is more, the global supply chain is also plagued by thieves, robbers, pirates, and hijackers. In fact, although policy makers have been mainly preoccupied with terrorism and trafficking since 2001, cargo theft has remained the top security concern for the private sector. Cargo theft causes substantial monetary, reputational, and social losses for cargo owners (shippers and consignees), logistics service providers (LSPs), and their insurers. In the European Union (EU) alone, yearly direct cargo theft losses exceed € 8,2 billion, which translates into an average loss of € 6,72 per carriage (van den Engel and Prummel 2007). Meanwhile, sea piracy costs the shipping industry between 7 and 12 billion dollars a year due to delays, detours, material losses, security expenditures, and ransoms (eyefortransport 2011). Another concern for the managers and the authorities alike is that robberies, hijacks and other violent forms of cargo theft jeopardize employee safety (IRU 2008).

International agreements and treaties set mandatory baseline requirements for the global SCS management and governance. Published in 2005, the SAFE Framework of Standards of the World Customs Organization (WCO) is perhaps the most important single SCS initiative introduced since 2001. Intended for customs administrations worldwide, the SAFE package offers a suite of best practices for maintaining adequate regulatory control over cargo flows while ensuring smooth cross-border commerce. Today, around 170 WCO member countries have "indicated their intention to implement" the standards of the most recent 2012 SAFE edition. The SAFE framework builds on two pillars of collaboration that have been inspiring SCS legislations around the globe: customs-to-customs coordination and customs-to-business partnerships. The customs-to-customs pillar seeks to harmonize rules for exchanging advance electronic cargo information (AECI)[1] between traders and customs, use of customs risk management, and inspection of high security risk traffic in the country of origin when requested by the customs in the country of destination. The customs-business partnership pillar rests largely on the voluntary Authorized Economic Operator (AEO) programs, in which customs grant simplifications to customs and/or security formalities for companies that have a good track record of compliance, are financially solvent, have a rigorous management processes

[1] The advance electronic cargo information (AECI) is also known as advance electronic information (AEI), and advance cargo information (ACI). I use the AEI abbreviation throughout the thesis.

in place, and that comply with minimum security requirements. The SAFE framework complements the WCO's older trade facilitation instrument Revised Kyoto Convention (RKC)[2] that aims to harmonize the disarray of customs formalities that hinder the international trade. The current edition of the Convention lays down best practices for improving transparency and predictability of the customs formalities. In particular, it dedicates special attention on the risk-based approach to border inspections and exchange of electronic information for efficient, automatic security risk assessment.

Supply chain security has been a key development area also for transportation authorities since 2001. In December 2002, motivated by the "9/11" attacks, the International Maritime Organization (IMO), a specialized body of the United Nations (UN), decided to create new minimum security requirements for protecting maritime supply chains against the threat of terrorism. The decision resulted in a fast development and adoption of the International Ship and Facility Security code (ISPS) that comprise mandatory security requirements (part A) and complementary guidance for implementation (part B). The ISPS code entered into force on the 1st of July 2004 as part the SOLAS convention (the International Convention of the Safety of Life at Seas) under the chapter XI-2 "Special Measures to Enhance Maritime Security." The inclusion of the ISPS-code into the SOLAS convention, an international treaty binding 159 signatory countries, facilitated global adoption of the new maritime security measures.

In the air transport domain, the International Civil Aviation Organization (ICAO), another specialized UN body, has been regulating the international civil aviation security since 1974 when it adopted the first edition of the Annex 17 to the Chicago Convention (Convention on International Civil Aviation). The Annex 17 (or its most recent edition) still defines "standards and recommendations" for "safeguarding international civil aviation against acts of unauthorized interference" in 191 signatory countries of the Chicago Convention. Right after the 9/11 disaster, the main focus of the civil aviation security has been evidently more on passenger security than on cargo security (recall air marshal programs, intensified passenger screening, and hardened cockpit doors). The air cargo mail security finally attracted wider interest in late 2010 when two explosive devices were discovered aboard aircrafts on two separate routings (more on this so-called "Yemen bomb plot" later). Soon after the discovery, the new edition of the Annex 17 introduced advanced security concepts such as the "secure supply chain" principle[3], and the consignment security declaration (CSD).

[2] The International Convention on the Simplification and Harmonization of Customs procedures

[3] In the secure supply chain air cargo (and mail) from trusted, certified shippers can be loaded on airplanes without extra security screening at the airport, if certain conditions are met. The consignment security declaration, states security status and other important details of air cargo (and mail) consignments. I describe the both concepts in detail later in this thesis.

Major institutional reforms took place in the years following the 9/11. In the US, in early 2002, the Homeland Security Act established the Department of Homeland Security (DHS), a body that took over key governmental functions involved in the US (non-military) counter-terrorism efforts. Later in 2003, the US Customs and Border Protection, a border security agency that assumed responsibilities of many formerly separate border control agencies, was created and annexed into the DHS. The same year, the DHS got responsibility for overseeing the Transportation Security Agency (TSA), a government body created in the aftermaths of the 9/11 attacks to oversee security of the US transportation, especially in the aviation domain. Meanwhile in the EU, the SCS agenda has been mainly driven by two Directorate Generals of the European Commission, the DG TAXUD (Taxation and Customs Union) and DG MOVE (Mobility and Transport).[4] The DG TAXUD takes care of customs related matters, and among other tasks, oversees the EU AEO program and customs coordination between the EU member states. The role of the DG MOVE, among other responsibilities, is to manage transport security across modes of transport. Other important EU bodies, involved mainly in operational, SCS include EUROPOL (European Police Office) for police forces, FRONTEX (*fr*. Frontières extérieures) for border guards, and EU INTCEN (European Union Intelligence Analysis Centre) for intelligence agencies. At the member state level, national authorities take responsibility for designing, implementing, and overseeing EU-level SCS legislations.

The global agreements and treaties are translated into practical requirements by national / regional governments. In the European Union (EU), important SCS-related regulatory advancements include the adoption of the ISPS code into the EU regulatory framework (725/2004) and the reform of the air cargo regime (300/2008/EC and 185/2010/EC), which introduced the "secure supply chain" concept, defined criteria for designating and screening high-risk cargo and mail (HRCM), and strengthened the principle of the rigorous 100 % air cargo screening. Another major EU regulatory reform is the "Safety and Security Amendment" of the Community Customs Code (CCC) (648/2005/EC and 1875/2006/EC) that introduced pre-arrival and pre-departure electronic declarations (so-called advanced electronic information dataset) to support early identification and control of security risks, voluntary Authorised Economic Operator Program (AEO) for facilitating cargo of trusted companies, and the rules for EU-wide, common criteria for identifying and targeting shipments that pose high security risk. The advance electronic (AEI) rules required traders to lodge electronic pre-arrival entry summary declarations (ENS) and pre-departure exit summary declarations (EXS) on the cargo prior to import or export from the EU customs security area (EU-28, Norway, and Switzerland)

[4] Before early 2010 the body responsible for transportation security was called DG TREN (Transport and Energy).

by transport mode-specific deadlines[5]. The AEI dataset enables customs in the EU customs security area to assess risk levels of departing and leaving cargo movements in advance before they cross the external EU borders. This early risk assessment enables the customs to identify, intercept, and eliminate security threats early in the supply chain. The EU AEO program sets the basis for partnerships between secure (and trusted) traders and customs, allowing the customs to concentrate limited inspection resources on unknown and/or non-trusted traders that, more likely than the AEO certificate holders, fail to comply with customs enforced law and regulations. The AEO-S (security and safety) and the AEO-F (Customs simplifications & security and safety) statuses allow the compliant companies to submit only a limited data set as part of the advance electronic information (EXS and ENS declarations), allows them to get prior notifications about customs controls under certain conditions, and subjects the trader to fewer security controls. The third key element in the "Safety and Security Amendment" is the introduction of the common, EU-wide risk assessment and uniform criteria for identification of shipments of high security risk. This reform set the basis for automatic uniform treatment of entering and exiting cargo consignments throughout the EU customs security area.

Way earlier than their EU colleaguaes, US policy makers the restructured government agencies got to handle an expanding number of SCS initiatives. The CPB was made responsible for the Container Security (CSI), which objective was and still is to screen US-bound shipping containers in foreign ports for security threats (mainly for nuclear and radioactive threats). The CPB became also responsible for C-TPAT (Customs-Trade Partnership Against Terrorist) program, the US equivalent of Authorized Economic Program (AEO). The agency also oversees two programs, the US "24-hour" rule and the more recent "10+2" rule (Importer Security Filing), that force shippers and logistics service provides to send the US authorities cargo information prior they load cargo on US-bound vessels. Later, to further strengthen the shipping container security, the US congress enacted a law "Implementing recommendations of the 9/11 Commission act of 2007" in August 2007, that required *every* US-bound maritime shipping container to be inspected at the last foreign port. Initially, this 100% screening legislation was meant to become operational by 1. July 2012, but due to a barrage of criticism from the private sector and other trading nations, and serious practical difficulties in implementing the regulation without crippling the seaborne transportation[6], the US Congress

[5] The advance electronic information (AEI) rule is sometimes misleadingly called the"EU 24-hour rule." The deadlines for sending AEI data set vary across modes of transport: 24h priort to loading for containerized maritime cargo, 4h before arrival at first port for bulk maritime cargo, by the time of take off for short haul flights, 4h before arrival at first airport for long haul flights, at least 2h before arrival for carried on rail and inland water ways, and at least 1h before arrival for road transport. (1875/2006, Section 3). The time limits are the ones in the WCO's SAFE framework of standards.

[6] One of the problems in the EU ports was that the ports might have X-ray and other screening devices, but the equipment is used mainly to check *imported* containers.

postponed the entry of the law by two years[7]. Outside the maritime context, TSA has been busy developing and implementing new air cargo and mail security legislations, most notably the 100-% screening requirement and the Known Shipper program.

Meanwhile, the business sector has been developing its own international and industry-wide SCS standards. The Transported Asset Protection Association (TAPA), a cross-industry business alliance committed to combat cargo theft, maintains three certifiable, voluntary industry standards: Freight Security Requirements (FSR), Truck Security Requirements (TSR), and the most recent TAPA Air Cargo Security Specifications (TACSS). It is important to notice that no mandatory anti-theft regulations exist, only voluntary industry-driven standards[8]. The certifications might be nevertheless necessary for carriers, cargo handlers, and warehouse keepers if they wish to make business with cargo owners that require top security from their logistics service providers. In fact, it is said that the voluntary SCS initiatives are becoming de-facto mandatory, as non-compliant companies are finding themselves in a competitive disadvantage vis-à-vis their compliant competitors (Hintsa et al. 2010b). Besides the standardization efforts, the TAPA lobbies for secure truck parking lots, dedicated cargo theft prosecutors, and harsher punishments for cargo thieves[9]. The business interest stems from the fact that a single truckload or a shipping container of electronics, medicines, trend apparels, or other high-value goods can be worth of several millions euros[10]. In Latin America, the Business Alliance for Secure Commerce (BASC), with the support the US Customs and Border Protection (CBP), maintains its own certifiable SCS program to counter smuggling, terrorism, and cargo theft (Gutiérrez 2007). The International Road Transport Union (IRU) promotes best practices for haulage companies to protect their cargo and employees from cargo crime and terrorism. Also the International Organization of Standardization (ISO) has developed a certifiable 28000 standard series around the ideas of continuous improvement and tailored, risk-based approach to SCS management.

The 9/11 attacks also spurred unprecedented academic research, giving a rise to the golden "post-2001" age of the SCS research (Hintsa 2011). Today, more than a decade of research later, SCS has secured its position as a standalone academic discipline (Williams et al. 2008), which

[7] Today, almost two years later, it seems that the Congress is forced to grant another two-year extension for the law.

[8] It is true that many requirements in government-driven SCS initiatives (e.g., C-TPAT, EU AEO) protect cargo from theft. But these government-driven SCS programs promote cargo integrity mainly to prevent terrorists from tampering shipments and introducing bombs or other weapons into the supply chain. The higher protection against cargo theft is a welcome side effect of the counter-terrorism measures.

[9] The authorities, especially the police, are interested in fighting cargo theft, but due to limited resources, the law enforcement is inclined to prioritize homicides, assaults over less violent property crimes such as cargo theft.

[10] Shippers, consignees, or their insurers pay bear the direct cost if a load gets stolen, and the governments lose tax revenues as thieves sell stolen goods without paying appropriate taxes. But eventually, consumers pay the bill of cargo theft as retailers must raise prices to offset cost of lost cargo.

studies exclusively supply chain risks that stem from intentional criminal activities (Ekwall 2009a). Research has been carried out under numerous rubrics, including supply chain security (Lee and Whang 2005), transport security (Urciuoli 2010; Haelterman 2011), and logistics security (Sheu et al. 2006; Sternberg et al. 2011). Nevertheless, despite the surge in the academic interest, earlier literature reviews characterize the SCS discipline as a fragmented and nascent field that lacks empirical studies (Williams et al. 2008; Voss et al. 2009a) and that has largely failed to map research into practical actions (Hintsa et al. 2009). A sign of the infancy of the discipline is that no formal definitions of the SCS management exist. Lacking a better one, many academics[11] acknowledge the statement of Closs and McGarrel (2004, pp. 8) as the de facto definition for SCS management:

> "Supply chain security management is the application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain."

We should always keep in mind that best estimates on criminal activities are no more than rough educated guesses that are often constructed with incomplete and doubtful data and that are sometimes corrupted by political agendas. The debate over the size of the illicit trade illustrates this difficulty of coming up with undisputable estimates of the criminal activity. In his book, Moises Naim (2009), an ex-editor in chief of the Foreign Policy magazine, warns about a new wave of transnational crime and terrorism that will destabilize the global politics. He asserts that technological advancements of the 1990's have created completely new lines of illegal trade (e.g., synthetic drugs) and enabled long-distance shipping of new types of contraband (e.g., human organs for transplants). He continues that free trade reforms and constantly reducing shipping and communication costs have shrunk the globe and expanded markets for illegal and legal goods alike. Meanwhile, whereas criminals and terrorists exploit the increased cross-border mobility to pursue business opportunities, national borders still handicap the international law enforcement. By contrast, one of the skeptical voices, economist R.T. Naylor (2007), remarks that there is no evidence to support the claim that the growth of the illicit trade is outpacing the growth of the legitimate commerce. He argues that the share of the illicit traffic of the total cross-border trade is in fact reducing because of higher transparency on international cargo flows and more relaxed trade and fiscal regulations. He points out that perhaps the most accurate proxy of the illicit trade is the amount of dirty money in the financial system. Based on a systematic meta-analysis of studies and statistics sources, the United Nation's Office on Drugs and Crime (UNODC 2011) estimates that proceedings of drug trafficking and organized crime amount for from 2,3 to 5,5 percent of the global

[11] At least Autry and Bobbit (2008), Voss et al. (2009b), Yang and Wei (2013), Sternberg et al. (2012) and Williams et al. (2009) cite the definition of Closs and McGarrel (2004).

GDP. The estimate is in line with view of the director of the International Monetary Fund (IMF) estimated that dirty money circulating in the global financial system amounts between 2 to 5 percent of the global economy. The UNODC's estimate, however, is significantly lower than the estimate of "experts," summoned together by the World Economic Forum, who presented that illicit trade accounts for 7 to 10 percent of the value of the world trade (WEF 2012).

Box 1 Estimates of illicit trade

1.2. Problem statements, motive, and research questions

This section elaborates the key problems of the supply chain security management that this doctoral research seeks to help solve. The section is split into three parts, each of which frames a one problem, discusses why academics and practitioners consider this problem important, and gives a brief outlook how this doctoral research is going to address the problem.

1.2.1. Confusion about supply chain security risk

Practitioners across industries, logistics functions, and government agencies tend to understand the notion of supply chain security risk in different ways. For transportation authorities in general, security risks are primarily associated with terrorist attacks on and through the transportation and logistics networks (DG MOVE 2013). On the other hand, customs administrations, which enforce security across all modes of transport, consider security threats as anything that could injure, kill, or otherwise damage, while moving through the supply chain. At the same time, people concerned with air cargo and mail security think that "assembled incendiary and explosive devices" count as security threats because only such devices may destroy aircrafts if loaded aboard aircrafts among airfreight and mail. Their thinking in turn differs from the perception of maritime authorities that see security risks mainly as the threat of concealed radioactive material or weapons in shipping containers. Furthermore, the security notion of the private sector operators differs fundamentally from the view of the authorities. In general, cargo owners – shippers and consignees – tend to associate security risks with cargo theft rather than terrorism and smuggling. Industry associations, such as IRU and TAPA, have raised concerns about violent hijacks and robberies that endanger driver safety and cargo integrity. The theft-orientation is evident in the TAPA's air cargo *security* standard (TACSS), which largely ignores cargo screening, that is a key element of any governmental air cargo security regulation. Instead, the standard offers a set of pure anti-theft measures, including "searches or inspections performed on *exit* from secure areas used for cargo; vehicle immobilization devices utilized; and […] provide robbery response training." Certainly, in many industry sectors, terrorism-related threats are considered high priorities. In the pharmaceutical, food, and other industries, where product contamination may kill people

and cause massive reputational damages, the risk of malicious product tampering is among the top-priority security risks.

The practitioners' views on supply chain security risks are diverse, inconsistent, and confusing. If the supply chain security risks covered the terrorism-related activities only, which seems to be the common understanding among the customs and transport security authorities, then cargo theft, a key security concern for the cargo owners and the logistics service providers (LSPs), would not technically be a "security risk." Problems of defining a concept as ambiguous as terrorism creates even more confusion. Generally, terrorism can be understood as something that employs violence and intimidation for advancing political or ideological goals. As the political motive is an inherent characteristic of terrorism, under the common understanding, if saboteurs were financially and not politically motivated, malicious product contamination would not be "terrorism" and therefore would not count as a "security risk." The link with terrorism with the supply chains is even a more complicating issue. Terrorists may exploit commercial supply chains, for instance, by stealing hazardous cargo, hijacking vehicles, dispatching weapons through the supply chain, or attacking directly supply chains structures. But many times the very same offences are committed for reasons other than political.

Unfortunately, the academic literature does not clarify the practitioners' confusing terminology. The literature provides some ad hoc characterizations of security risks, but the current body of knowledge lacks a profound theoretical discussion on what kinds of risks the SCS management address. A commonly cited definition of Closs and McGarrel (2004) considers that the SCS management tackles "theft, damage, or terrorism, and […] the introduction of unauthorized contraband, people, or weapons of mass destruction in the supply chain." As part of a common review of supply chain risks, Manuj and Mentzer (2008) suggest that security risks cover "freight breaches, terrorism, vandalism, crime, and sabotage." Williams et al. (2009a) point out that the SCS management generally protects the supply chains from "damage, terrorism, and contraband." All the same, the main problem of these apparently ad hoc academic definitions is that they treat terrorism, security threats, damage, and crime as if these concepts were distinct and comparable varieties of supply chain risks. The doctoral research of Ekwall (2009a) is one of the few works that classify security risks into distinct categories and that thus elevate the discussion to a more theoretical level. The Ekwall's motivation-based classification groups the security risks into profit-driven crimes (e.g., theft and trafficking), non-profit-driven crimes (e.g., terrorism and sabotage), and crimes that co-occur with the profit and non-profit crimes (e.g., corruption and fraud). However, the classification comprises three largely overlapping categories: theft and trafficking can be committed also for non-profit reasons (e.g., theft and smuggling of radioactive material may be linked to terrorism) and sabotage can be committed for profit (e.g., blackmailing associated with product contamination). Moreover, it appears that

the classification is not constructed following a systematic method or on the basis of empirical data.

Altogether, the extant SCS literature offers only a cursory and rather confusing look on the risks that the SCS management addresses. A few ad hoc definitions and classifications exist, but no earlier studies explore the SCS risks methodologically, following a rigorous and transparent research procedure and/or using empirical evidence. The lack of rigorous classifications is particularly astonishing because many *researchers* consider identification of sources of risk and uncertainty as the first step in managing the risk in the supply chain context (Sodhi et al. 2012). This fundamental weakness has serious implications: without a unifying classification, boundaries of the SCS discipline remain blurred, making it difficult for SCS scholars to position their research in the context general supply chain risk management. Furthermore, due to the unspecified sources of security risks, the practitioners cannot apply risk matrices, risk registers, and other analytical risk management tools to the maximum effect. In general, the lack of common vocabulary among the supply chain practitioners undermines efforts for cross-industry benchmarking and sharing of best practices. Given the diversity of views on the SCS risks, the academics and the practitioners alike would benefit from a crime risk classification that would offer a global view on the security risks that occur in the supply chain context.

In this dissertation, I develop supply chain crime taxonomy, which seeks to identify, characterize, and categorize risks that SCS management addresses. This taxonomy is to be developed empirically based on written and verbal accounts of senior managers on crime risks that occur or could occur in the supply chains they manage. The taxonomy development is guided by the following research question: **What risks does supply chain security management address?**

The taxonomy would strengthen the weak ontological foundations of the SCS discipline, by clarifying the confusing terminology, capturing supply chain crime under a unifying theoretical frame, and carving boundaries for the theory and practice of the SCS management. The identification of specific crime types would set a solid foundation for further crime type specific studies. Classifying the crime types by "criminal intervention" (i.e., the way criminals interact with the supply chain) would help the practitioners tailor preventive security measures that reduce crime opportunities, discourage potential offenders, protect cargo integrity, and facilitate criminal investigations. The main academic motive for the taxonomy development arises from the call of Hintsa (2011) for research pursuing "in-depth understanding" of supply chain crime types. The taxonomy research also answers to the call of Jüttner et al. (2003) on more research on risk sources that give arise to risk outcomes in the supply chain context. The taxonomy complements and refines also earlier academic taxonomies on general supply chain risks (e.g., Kleindorfer and Saad 2004; Jüttner et al. 2003; Manuj and Mentzer 2008).

1.2.2. Debated effects of supply chain security

The protection of cargo flows from pirates, bandits, and other criminals has been the main purpose the SCS management since the early days of trade and commerce. Today, security is still about getting cargo reliably from A to B so that the trade can prosper despite crime threats that overshadow the global logistics. All the same the protection the supply chain crime comes at a cost: in addition to direct spending in security equipment, training, and operations, SCS solutions tend to complicate and slow down day-to-day logistics. Cargo inspections many times disrupt optimized logistics processes at seaports (Bakshi et al. 2011), border crossings (Voss et al. 2009a), and at airports (ICAO-WCO 2013). Access to logistics facilities gets delayed due to time-consuming entry protocols that involve waiting, document handling, and conversations with gatekeepers (Sternberg et al. 2012). Security-influenced routing around criminal "hotspots" implies costs, delays, and extra coordination (Reilly et al. 2012; Murray-Tuite and Fei 2010). Regulatory responses to security breaches, such as traffic suspensions, evacuations, and increasingly stringent screening requirements, may disrupt logistics more than the actual security breaches (Sheffi 2001).

The academic literature suggests that there might be certain win-win solutions that would bring more security and/or logistics benefits with few resource investments. Inspired by the Total Quality Management (TQM) philosophy, Lee and Wolfe (2003) and Russel and Saldanha (2003) propose for example that we could reach higher security of the supply chain at a low cost by securing cargo at origin, ensuring in-transit cargo integrity throughout the supply chain, and making security anyone's business. Another stream of literature advocates collaboration across business partners and government agencies as the way towards logistics and security excellence (Sheffi 2001; Closs and McGarrel 2004; Sarathy 2006; Russel and Saldanha 2003; Manuj and Mentzer 2008; Autry and Bobbit 2008; and Williams et al. 2008). A third research stream considers security culture – something characterized by vigilant employees who are willing and able to prevent and detect security breaches – as the key for reconciling the conflict between the security and logistics goals (Voss et al. 2009a; Autry and Bobbit 2008; Rice and Caniato 2003; Martens et al. 2009).

But after all, the literature on the effects of the SCS implementation on the SCS performance and the logistics performance seems rather scarce. Few plausible yet untested theoretical arguments exist, but it is unclear why, to what extent, and under what conditions the SCS implementation affects the security and the logistics performance. The apparent lack of the SCS knowledge is surprising given the heightened interest in the SCS research since the 9/11 disaster. If the 9/11 attacks started the golden age of the SCS research, why do earlier SCS literature reviews include mostly general risk management studies in their sample (Voss et al. 2009a; Williams et al. 2008) and not SCS-specific studies? Should not scholarly journals have observed a surge in SCS

manuscripts over the past decade? Is the apparent small number of SCS studies due to the journals' aversion to the SCS research or due to the fact that we have not considered all outlets of academic SCS research. The latter alternative seems more plausible. In fact, there might be a large body of SCS knowledge buried in numerous studies that are scattered across a broad range of academic journals.

My hypothesis is that principles for logistics-friendly design of security systems exist, but because of the interdisciplinary nature of the SCS research, these bits and pieces of knowledge are difficult to find and reconcile. In this dissertation, I will identify and synthetize relevant earlier SCS research that help us understand better the relationship between the security implementation, the security performance, and the logistics performance. To do this, I employ the so-called systematic literature review (SLR) method, an approach following a prescribed, reversible process of searching, analyzing, and synthetizing various research products: theoretical arguments, empirical evidence, and analytical reasoning. The resultant synthesis, a study of studies, offers the most powerful evidence for discussing the existence of potential logistics-friendly security design principles. Formally, the synthesis aims to answer to the question: **What principles do underpin design of logistics-friendly security systems?**

Based on my numerous conversations with logistics managers, security experts, and authorities, I found that practitioners would highly value prescriptive, evidence-based guidance for designing logistics-friendly SCS systems. The academic motive for the research arises from the call of Ekwall (2009a) and Hintsa (2011) for research on implications of SCS on logistics performance. The use of the SLR technique for exploring the extant body of knowledge is motivated by the criticism towards poor quality of traditional, narrative literature reviews in the management research in general (Tranfield et al. 2003) and in the supply chain management research in particular (Seuring and Gold 2012). The pointiest critics accuse the traditional narrative literature of being biased ad hoc accounts of selected publications that tend to support reviewers' subjective preconceptions (Rousseau et al. 2008).

1.2.3. Swiss Post case study

After the development of the supply chain crime taxonomy and the model for logistics-friendly SCS management, there is need to validate these theoretical frameworks by assessing how accurately they reflect the reality where modern logistics networks are embedded. For this validation purpose, the third research phase constructs a case study of the Swiss-centric international postal network. The case study description is to exhibit how the postal logistics and associated security activities function in practice. The subsequent case study analysis applies the crime taxonomy and the model for logistics-friendly SCS to the case study context.

The analysis also seeks to identify evidence-based concepts for improving the postal security in Switzerland and elsewhere.

Why does the case focus on the postal logistics? A key reason for the focus is that the postal logistics represent a relative simple microcosm of the complex global freight logistics network. That is to say, postal operators are a somewhat homogenous group of logistics actors, which offer more or less same services, operate under a single global framework of standards, follow comparable logistics processes, encounter similar security problems, and for the most part control the end-to-end postal logistics network. By contrast, the variety of freight logistics operations is much broader in terms of business models, logistics practices, standards and regulations, and so forth.

Another reason to focus on the postal logistics is the topicality of postal security management. Recent and foreseen regulatory changes imply that the postal security management is undergoing its biggest reform in modern times. In 2012, for the first time in history, the Universal Postal Union (UPU), the United Nations (UN) organization coordinating global postal policies, made requirements of its two postal security standards globally binding, for all of its 192 members countries. From that moment onwards, the two standards, one on general postal security (S58) and the other on airmail security (S59), have set minimum security requirements for the global postal service. Also regional legislations have been rapidly evolving over the past few years, with major implications on the postal security. In the EU, the framework regulation (300/2008) and its implementing regulation (185/2010) set unprecedentedly stringent security requirements for air cargo and airmail security in the EU aviation security area[12]. The later amendment (859/2011) expanded the EU air cargo and airmail security regime to cover airlines operating from third country airports. The amendment also specified criteria for identifying and screening high-risk cargo and mail (HRCM). Today, the EU is about to reform its customs security legislation framework again. Back in 2005, as part of the Customs Code Safety and Security amendment (648/2005 and 1875/2006), the EU introduced rules for advance electronic information (AEI), which enabled customs administrations in the EU to identify, and in some cases examine, high-risk shipment before they entered or exited the EU territory. The postal traffic is currently exempted from AEI provision, but this exception, at least in certain segments of the postal traffic, is likely going to be revoked as soon as the new Union Customs Code becomes applicable.

Business developments also indicate the mounting interest in the postal security management. Postal operations have launched new product lines, including real-time tracking & tracing, extra insurance coverage, and supplementary bomb screening to meet growing demand for

[12] The EU aviation security area covers the 28 EU member states, Switzerland, Norway, and Iceland.

security services. At the same time, consultants, technology companies, and security firms offer an increasing number of products around the postal security theme, award prizes for leading "security innovators," and publish reports and educational material on the topic. The global industry collaboration is lead by the UPU or technically its newly established security collaborative called Postal Security Group[13]. Regional postal lobbies have set their own security task forces, such as the Strategic Security Task Force of PostEurop, an association representing 43 public postal operators in Europe. PostEurop also coordinates the SAFEPOST project that brings together a large number companies, authorities, scholars, and consultants from multiple countries and disciplines to develop new generation solutions for addressing crime in the international postal network. The four-year project, funded by the European Commission (EC), has a budget of close to 15 million € and is expected to create "sustainable total postal security solutions encompassing organizational, process, technological, human factors and training perspectives."

Recent terrorist events and crime trends stimulate the debate and the activity around the postal security management. In October 2010, al-Queada terrorists almost succeeded to destroy two airplanes with a pair of Yemen-origin express courier parcels, each enclosing plastic explosives hidden inside a printer toner cartridge. This "Yemen bomb plot" was eventually foiled, largely thanks to a timely piece of intelligence and prompt interventions from the side of authorities. Even so, before the parcel bombs were intercepted at stopover airports in England and Dubai, they had travelled aboard three passenger planes and two air freighters. The postal industry fairly reminds that the bombs travelled in the express courier channel, outside the *postal* network. But despite this fact, the events reminded the vulnerability of the airmail logistics to terrorist exploitation. The fallout of the Yemen bomb plot is not however driving the postal security agenda alone. News on mail bombs and ricin-laden letters demonstrate that terrorists exploit the postal service to attack their targets from distance. Also the threat of bio-terrorism is looming over the postal service still today, more than a decade after the infamous Anthrax attacks in the US, which killed five people, only a few weeks after the "9/11" tragedy. Moreover, concerns have been raised that the international postal system is used to smuggle drugs, firearms, doping substances, counterfeits, and dirty money – or basically any illegal commodity compact enough fit a parcel or an envelope. The problem is that the illegal traffic through the postal system appears to be growing hand in hand with the proliferation of rogue online pharmacies, replica stores, and black markets that use the postal service to ship their illegal merchandise to clients, like legitimate online merchants. On top of the heightened risk of

[13] UPU has been active in postal security since 1989, when it established the Postal Security Action Group, the predecessor of the Postal Security Group, to foster international security collaboration and standard development.

terrorism and smuggling, mail theft is still a top security concern for postal operators worldwide, especially when it comes to robberies and other violent methods of stealing mail.

The postal industry is committed to fight crime and terrorism, but not at any cost. The industry position is that postal security should "make business sense" – improve rather than deteriorate the quality of the postal service. Alas, the postal sector faces the same dilemma than many other industries. On the one hand, the postal security reduces theft, smuggling, and terrorism, and thus lowers the risk of crime-triggered disruptions of the postal service. In other words, security increases chances that the right piece of mail gets delivered to the right address by the promised day. On the other hand, security procedures tend to complicate the routine postal logistics operations, making the day-to-day mail delivery slower, less predictable, and more expensive. The complicating effect of security is most obvious in the international postal service, which is disproportionally costlier, slower, and more uncertain than the domestic service. As a point of reference Table 1 compares the Swiss domestic first class letter service to the international first class letter service between Switzerland and its two neighboring countries France and Italy. We find that the international delivery costs 4,3 times more for the sender than the domestic delivery. The finding is consistent with Okholm et al. (2010) who point out, based on a much larger sample, that the intra-EU cross-border postal delivery costs typically three to five times more than national delivery. Moreover, the international letter to Italy is delivered in two to four days while the domestic letter reaches its addressee next working day. Longer distances explain partly the striking differences in terms of cost, speed, and uncertainty between the cross-border and the domestic postal services. The price difference can be explained further with characteristics of the international postal logistics, including weak competition, relatively low traffic volumes, and involvement of a high number of logistics actors. Nevertheless, despite all these reasons, the security procedures and border formalities have evidently much to do with the disparity between the international and domestic services. Consider that the international postal traffic is subject to customs controls in the country of origin, in the country of destination, and possibly in one or more transit countries. Airmail is subject to security and safety screening. These security and border controls cost money and often delay the mail delivery process.

	Domestic A letter (100g)	International Priority letter (100g)	
Origin → destination	CH → CH	CH → France	CH → Italy
Postage (CHF)	1,00	4,30	4,30
Delivery time (working days after posting)	1	2-3	2-4

Uncertainty of delivery time (days)	0	1	2

Table 1 Illustrative comparison of international and domestic postal services (Source: Swiss Post)

The postal service has potential to dominate the low-cost segment of e-commerce shipping services, where customers generally value inexpensive service over fast and day-certain delivery. Nevertheless, if the Posts want to fully capitalize on the growing cross-border market, that is projected to grow by 75% from 2010 to 2020 (IPC-BCG 2012), the Posts must provide a wider range of services that online retailers and shoppers demand. Market research suggests that high costs and long delivery times are the most common reasons why the online shoppers abandon their virtual shopping carts without placing orders (Okholm et al. 2013). The European Commission (2014) states that delivery-related problems, including long delivery times and high and uncertain costs, account for "almost 70% of abandoned online shopping transactions." The online shoppers and retailers demand reliable shipping services that deliver goods consistently within day-definite time windows (IPC 2013). The problem is that while the shoppers and the retailers trade in the borderless online environment, the physical postal delivery still gets delayed at borders due to customs and security controls. Deeper integration of the security and customs controls into the sequence of the postal logistics process would speed up the logistics and make it more predictable. The integration would allow Posts to offer a wider range of delivery services, such a day-certain or time-definite delivery, that would better match preferences of the online shoppers and retailers.

Post may also lose money due to substandard on-time delivery performance. The EU's Postal Directive (97/67/EC) sets two performance objectives for the intra-EU cross-border postal service, that apply for each bilateral mail flow between two member states. Meeting the speed objective requires that 85% of cross-border priority letters get delivered within three days after the day of posting (D + 3). The reliability objective states that 97% of the priority letter traffic should arrive within five days from posting (D + 5). Although the objectives are called "speed" and "reliability," they are both measures of on-time delivery performance. More ambitious performance objectives are set by the REIMS agreements (Remuneration of International Mail), which current fifth edition REIMS V lays down rules for inter-Post price transfers, called terminal dues, between 24 European postal operators[14]. The REIMS III agreement set a target that says that 93% of the first class letters should to be delivered next day (D + 1). A key principle in the REIMS system and the Postal Directive is that "quality," in terms of on-time delivery performance of first class letters, should affect the terminal dues, in addition to weight-

[14] According to the latest update on www.ipc.be/en/Operational-services/Intercompany_pricing/REIMS_V. Accessed 18. June 2014.

based costs of handling and delivering foreign-origin traffic. Accordingly, poor performing Posts lose money, as they receive less terminal dues as a penalty for inferior delivery speed.

To conclude so far, all signs indicate that the fast, reliable, and inexpensive cross-border logistics is no less than a strategic necessity for Posts that are redefining their role in the modern economy, characterized by the declining mail volumes, intensifying competition, and the heightened security concerns. Excellent logistics capabilities would enable Posts to launch services that the e-commerce customers demand, compete head-to-head with the express couriers, and capitalize on the growing cross-border e-commerce that is driving demand for small packets and parcels. The excellent logistics capabilities would also help avoid monetary penalties of inferior on-time delivery performance. Alas, security and customs procedures tend to disrupt the routine postal logistics processes and especially the cross-border postal service. Given all the security and business challenges the postal industry is facing today, there is a definite need to develop solutions for securing the postal service with lowest negative impact on the postal logistics performance.

However, despite the relevance of the postal security management for the contemporary postal industry, academic research on the postal security is at an early stage. Only a handful journal papers, conference proceedings, and dissertations discuss security and crime in the postal logistics context. The thesis of McCarthy (2009) outlines security governance and management practices at the Royal Mail, with focus on theft and terrorism. Building mainly on anecdotal evidence, Hintsa et al. (2010a) link postal security to a general theory of the SCS management. The *Journal of Contingencies and Crisis Management* has an issue on the Anthrax threat to the postal service. But that is all: the body of knowledge is scarce. Therefore, to augment the scant literature, this dissertation presents a descriptive case study on the Swiss-centric postal logistics network, putting a spotlight on postal crime and postal security management practices. The subsequent analysis of the case evidence aims at identifying evidence-based concepts for improved postal security management. The formal research question for the case study is: **How to secure the international postal service without disrupting the routine postal logistics processes?**

Overall, there is a practical need for descriptive, positive research that allows different stakeholders to benchmark their current approaches to the postal security management. Practitioners are also looking for scientific, normative guidance for making more insightful decisions on the postal security matters. The case analysis seeks to primarily to help Swiss Post and Swiss authorities to update their approach to postal security. However, some findings and recommendations are likely to be applicable also beyond the Swiss context. Thus, it is possible that case study findings might bring global benefits for the postal sector and the users of the postal service. In fact, even incremental improvements to the global postal service might yield substantial benefits over time if the improvement affected billions of international postal

shipments that postal operators deliver each year. The case study research also contributes to the implementation of the general postal security strategy of the Universal Postal Union (UPU) by increasing general awareness about the relevance of the postal security. In this respect, in particular, the research provides tools and solutions for intensified timely sharing of "operational, security, and investigative information" among key stakeholders of the postal logistics. The case study research also complements the limited body of empirical case-based studies in logistics (da Mota Pedrosa et al. 2012), supply chain risk management (Jüttner et al. 2003), and supply chain security (Voss et al. 2009a). The research also answers to the call of Manuj and Mentzer (2008) for research on managerial SCS strategies and the call of Williams et al. (2008) for research on linkages between SCS implementation and organizational performance. The research also enriches the academic debate on motives for SCS implementation (Williams et al. 2009a; Bakshi et al. 2011; Prokop 2012).

1.3. Structure of the thesis

This section outlines the structure of this thesis so that readers can easily navigate through the eight chapters of the dissertation and find quickly information they are looking for. The thesis is structured around three interconnected studies, each of which I plan to publish in a medium-to-high rank academic journal.[15] Chapter 4 produces a supply chain crime taxonomy that identifies, charactrizes, and categorizes risks that the SCS management addresses. The second study, the systematic literature review, is presented in chapter 3. It seeks to identify themes and principles of logistics-friendly SCS management. The third case study spans chapters 5 and 6, and it aims to come up with concepts for improving postal security management. The remaining three chapters (1-2 & 7) supply the readers with necessary background information that allow them to judge credibility, relevance, and contribution of these three studies and thus the entire PhD thesis. Each chapter is briefly introduced below.

Chapter 1 – Introduction. The introductory chapter frames the context of the post-2001 SCS research and practice by highlighting its key debates and challenges. After a brief outlook to the central SCS themes, the chapter describes research problems, formulates research questions, and explains academic and practical motivations for the research.

Chapter 2 – Methodology. The second chapter elaborates and justifies methodological choices that underpin the research of this PhD work. Detailed descriptions of sampling strategies, research methods, and quality safeguards allow the readers to judge credibility of the findings

[15] The first study on the supply chain crime taxonomy (Ch. 4) has already been published in the *International Journal of Shipping and Transport Logistics*. Other two studies, the systematic literature review (Ch. 3) and the case study (Ch. 5-6), still wait to be converted into a form of a publishable research article.

and conclusions of this dissertation. The last sections of the chapter discuss measures taken to protect information sources and to prevent abuse of the findings of this security-related research findings for illegal purposes.

Chapter 3 – Systematic literature review. The chapter characterizes and synthesizes SCS that have been published in peer-reviewed academic journals since 2001. Building on the literature synthesis, the chapter discusses what SCS solutions are, redefines dimensions of SCS performance, and summarizes effects of SCS implementation on the SCS performance and logistics performance. The final part of the chapter sets lays down principles of logistics-friendly design of SCS systems.

Chapter 4 – Supply chain crime taxonomy. This chapter starts with a brief review of the academic literature that aims to identify key characteristics of supply chain security (SCS) risks. Building on this characterization, the chapter analyzes managerial perceptions on crime problems that occur or could occur in the supply chain context. These managerial views on the supply chain crime problems are then used to develop a taxonomy of supply chain crimes. The chapter concludes by assessing the validity of the taxonomy by applying it to the context of the Swiss-centric international postal logistics.

Chapter 5 – Case study description. This first descriptive case study chapter depicts the current state of the international postal service from the Swiss perspective, putting a special emphasis on supply chain security and law enforcement. The chapter starts with an introduction to Swiss Post and its core postal operations before proceeding into details of postal security management in the Swiss-centric cross-border postal service. The last section wraps up the case study description by mapping the identified postal security domains onto the baseline postal logistics process.

Chapter 6 – Case study analysis. Building on the previous case study description and systematic literature chapters, the case study analysis seeks to identify evidence-based concepts for improving the postal security management. The analysis applies the design principles of logistics-friendly supply chain security management as the theoretical basis (Ch. 3) and the case study evidence as the empirical bedrock (Ch. 5). The chapter concludes by summing up key findings and recommendations to the postal security management and governance in Switzerland, in the European Union, and worldwide at the Universal Postal Union level.

Chapter 7 – Conclusions. The final chapter opens with a brief summary of the main research findings, conclusions, and recommendations. It proceeds to discuss how the findings of the PhD project contribute to the theory and the practice of the SCS management. Next the chapter elaborates generalizability of the conclusions and recommendations beyond the study's immediate research context. Concluding the whole thesis, the chapter highlights promising key topic areas and methodological considerations for future supply chain security research.

Summary

This chapter introduced key debates, regulations, initiatives, and institutional developments that define the theory and the practice of the post-2001 supply chain security (SCS) management. After the brief instruction, the chapter described how this doctoral thesis seeks to strengthen the theoretical underpinnings of the SCS discipline by developing a supply chain crime taxonomy and by consolidating a model for logistics-friendly design of SCS systems. The chapter provided an outlook to the case study on the Swiss-centric postal logistics network that is later used to test the supply chain crime taxonomy and the model for logistics-friendly SCS design in practice. The chapter concluded by outlining the structure of this document.

Chapter 2 | Methodology

This chapter describes and justifies methodological choices taken in this PhD project and discusses their implications to research quality. This account helps readers judge methodological rigor and thus credibility of findings and conclusions of this dissertation. The chapter clarifies first philosophical tenets underpinning the research before proceeding to detailed elaboration of strategies of inquiry, research methods, and data. The chapter concludes by discussing research ethics and evaluating strengths and weaknesses of the overall research design.

2.1. Philosophical worldview

A worldview, defined as "a basic set of beliefs that guide action" (Guba 1990), determines philosophical assumptions that underpin selection of methods and strategies of inquiry. Scholarly literatures calls worldviews also as paradigms, epistemologies, and broadly conceived methodologies (Cresswell 2009). I discuss here briefly two dominant worldviews – postpositivism and constructivism – and explain why I decided to follow the latter in this doctoral research.

The post-positivism worldview, often referred as the scientific method or empirical science (Creswell 2009), assumes that the world exists independent of the observers, but researchers can never capture the absolute truth (Phillips and Burbules 2000). The worldview rests largely on the hypothetico-deductive reasoning in which scientists derive hypotheses on causal relationships from theory and test them empirically through a meticulous measurement of hypothetically related variables. The scientists refine, revise, and abandon their theories in the light of new empirical evidence. The constructivist worldview holds that the reality is a fabric of socially constructed and contextually embedded meanings (Crotty 1998), and that the aim of the scientific inquiry is to understand this inter-subjective reality. Constructivists acknowledge that objective research is an elusive ideal, as any research activity invariably shape, if not distort, the reality it tries to understand. The constructivism is inclined towards qualitative strategies of inquiry (e.g., case study and ethnography) and methods (e.g., questionnaires with open-ended questions) that aim to understand real-world, often social, phenomena in-depth by gathering

fine-grained contextual insights (Creswell 2009). The worldview allows hypothesis-generating data-driven theory building (Glaser and Strauss 1967).

This thesis follows the constructivist worldview for three reasons. First, previous research has barely scratched the surface of the research problems this thesis addresses. It has been said that an unexplored research topic justifies the use of the qualitative research techniques that, in the spirit of the constructivism, lay the basis for profound situational understanding (Miles and Huberman 1994). Second, previous reviews of more experienced scholars (Williams et al. 2008; Voss et al. 2009a) and my own precursory literature review (Männistö 2011) indicate that the supply chain security (SCS) discipline rests on a rather weak theoretical basis. The qualitative strategies and methods the constructivist worldview advocates are suitable when research aims to incrementally reinforce theory in a nascent discipline (Edmondson and McManus 2007). Third, earlier research (e.g., Urciuoli 2010) and my own experiences suggest that given security sensitivity of data, companies and authorities do not always compile security and crime statistics and if they did, they would be reluctant to share this data with researchers. The lack of access to quality numerical data effectively impairs ambitions for the hypothesis testing quantitative research.

2.2. Overview of research design

This section elaborates methods, strategies of inquiry, and criteria for assessing quality of research that all stem from the constructivist philosophical worldview. This doctoral study comprises three interconnected studies[16]. Each study employs variant strategies of inquiry and methods to tackle their distinct yet connected research problems. In this document, the strategies of inquiry refer to the "types of qualitative, quantitative, and mixed methods designs or models that provide specific direction for procedures in a research design" (Creswell 2009, pp. 11). Scholars have called the strategies of inquiry also as research methodologies and approaches (Cresswell 2009). The methods shall refer to specific techniques used to collect and analyze data as well as to validate and report findings.

The first one of the three studies is called supply chain crime taxonomy. In this study, my colleagues and me sought to identify, define, characterize, and classify crime activities that occur or might occur in the context of international commercial supply chains. To meet this goal, we asked a group of eighteen managers to describe their views on crime problems in the supply chains they manage. The sample of eighteen managers consisted of senior level managers from relatively large international companies (> 500M€ sales) across a variety of industries. To elicit the crime problems, we employed semi-structured one-to-one interviews,

[16] My ambition is to publish each study eventually as a research article in a peer-reviewed academic journal. The first study on the supply chain crime taxonomy (Ch. 4) has already been published in *International Journal of Shipping and Transport Logistics*.

semi-structured group interviews, and self-administered surveys with open-ended questions. The selected strategy of inquiry can be best characterized as the phenomenological approach in which "the researcher identifies the essence of human experiences about a phenomenon as described by participants" (Cresswell 2009). The crime taxonomy surfaced when I analyzed the crime descriptions with a content analysis technique. Finally, the case study on the Swiss-centric postal logistics network was used to test the validity of the taxonomy.

In the second study called systematic literature review, I aimed to construct a model for logistics-friendly SCS management and to set an agenda for future research. Like the name of the study suggests, the research was conducted following a literature synthesis technique called systematic literature review (SLR). The technique follows a prescribed and transparent procedure that is devised to reduce researcher bias and enable readers judge the credibility of findings and conclusions (Denyer et al. 2008). This systematic technique is different from the traditional narrative literature reviews that are criticized to be biased ad hoc accounts of selected publications that tend to support reviewers' subjective preconceptions (Rousseau et al. 2008). My precursory literature review revealed (Männistö 2011) that the SCS discipline is characterized by a multiplicity of research questions, methods, and theoretical perspectives. This diversity makes it impossible to use statistical aggregation to synthetize research findings (e.g., How to analyze qualitative data with statistical tools?). Therefore, my literature review applies so-called realist synthesis technique to make sense of the diverse scientific evidence (Denyer and Tranfield 2006). The technique of realist the synthesis is also ideal for building mid-range theories proposing "what works for whom in what circumstances" (Pawson and Tilley 1997).

The third research phase and the third study aims to describe the current state of the postal security management in the Swiss centric cross-border logistics network. For this study, case study approach was selected because the unit of analysis (the postal logistics) is a dynamic real-world phenomenon that cannot be properly understood without a deep contextual analysis. The choice of the case study approach is consistent with Yin (2009) who suggests that the case approach is appropriate when investigating "contemporary phenomenon in depth and with its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." As a bonus benefit, the case study approach gives researchers a freedom to select the most suitable methods for data collection and analysis and allows them to tap into multiple sources of evidence (Yin 2009). Such pragmatism helps build a rich, insightful case description that underpins consequent interpretations, conclusions, and recommendations.

This thesis culminates in the case study analysis chapter (Ch. 6). Building on the previous case study description and systematic literature chapters, the case study analysis seeks to identify evidence-based concepts for improving the postal security management. The case analysis gives

the first impression of the validity of the supply chain crime taxonomy and the model for logistics-friendly SCS management. To conclude this section, Table 2 summarizes the essential aspects of the three studies and research phases.

	Supply chain crime taxonomy (Ch. 4)	Systematic literature review (Ch. 3)	Case study (Ch. 5 - 6)
Research question	What risks does supply chain security management address?	What principles do underpin design of logistics-friendly security systems?	How to secure the international postal service without disrupting routine postal logistics processes?
Unit of analysis	Managerial descriptions of crime problems	Peer-reviewed research articles	The international postal logistics network from the Swiss perspective
Outcome	a) Taxonomy of supply chain crimes	b) Model for logistics-friendly SCS management c) Research agenda	d) Case description e) Evidence on validity of a & b f) Concepts for improving postal security management

Table 2 Summary of the three research phases

2.3. Research methods

This section elaborates and justifies research methods and techniques I have used to collect and analyze data as well as validate research findings and conclusions. The section has three sub-sections, one for each of the three research phases: the supply chain crime taxonomy, the systematic literature review, and the case study.

2.3.1. Supply chain crime taxonomy

The first study, the supply chain crime taxonomy, is based largely on data that my colleagues and me have collected during the yearlong LOGSEC project on logistics security[17]. At the outset of the data collection, we chose a sampling strategy. Because of the large number of Europe-based companies engaged in the cross-border logistics and transport, it was beyond the capabilities of the LOGSEC project to collect managerial descriptions of crime problems from a large enough sample of managers to enable statistical analysis. Therefore, instead of the random probability sampling, we decided to follow purposeful sampling, in which the research team

[17] The LOGSEC project, funded under 7th framework programme (FP7) of the European Commission, provided a strategic roadmap towards a large-scale demonstration project in European logistics and supply chain security.

identified and selected managers according to three criteria. First, the sample of managers was to include only managers working for companies generating over 500 million € of sales revenues per annum. Second, these companies needed to source and/or sell their products internationally. The reasoning for the first and second criteria was that internationally active major corporations are more likely to confront a larger variety of supply chain crime problems than domestically operating small and medium sized enterprises (SMEs). Third, all managers were required to have senior level positions in supply chain or corporate security functions. As the final general criterion, the companies of the selected managers needed, collectively, represent a broad variety of prominent European industries and functions in an international end-to-end supply chain. The research team approached the candidate companies via three major industry organizations: the European Shipper's council (ESC), which represents over 100000 cargo owners in Europe; the European Association for Forwarding, Transport, Logistics and Customs Services (CLECAT), which works for around 19000 Europe-based freight forwarders and customs agents; and Transported Asset Protection Association (TAPA), which nearby 300 members are mainly shippers and logistics companies involved in the logistics of high-value goods. The research team used their personal networks in these organizations to engage suitable managers in the study. Data collection took place between September 2010 and February 2011 as part of the LOGSEC project.

The final sample encompasses eighteen senior managers who represent Europe-based companies across a variety of industry sectors. The participants were given the choice to join in the study either by filling a survey or by participating one-to-one or group interviews. The informants' freedom to select their preferred way of participation likely increased their willingness to share their perceptions and experiences on the rather sensitive crime problems. Each of the three data collection methods posed an equivalent set of questions for the managers, though wording, combination, and sequence of the questions varied across methods to a degree. The data collection methods were based on a common study protocol to alleviate the risk of getting incommensurable data. As one of the group interview participants also submitted the survey, and another participated also one-to-one interview, a total of twenty responses were collected. Nine participants completed the survey form, six partook in one-to-one interview, and five joined the group interview sessions. During the data collection, the LOGSEC consortium arranged two group interview sessions that involved two and three managers, respectively. The data collection continued until the researchers realized that interviewing or surveying additional managers would reveal only little new relevant information. Table 3 presents the demographics of the respondents and a summary of the applied data collection methods.

	Respondents by method	
	Total	

Respondents by industry sector	Responses	Self-administered survey	One-to-one interview	Group interview
Aerospace	1	1	0	0
Automobile	1	1	0	0
Beverages	1	0	1	0
Chemicals	1	0	0	1
Communication/electronics	7	3	2	2
Food wholesale/retail	1	0	1	0
Logistics service providers	2	2	0	0
Machinery	1	0	1	0
Pharmaceuticals	4	1	1	2
Textile	1	1	0	0
Total	20	9	6	5
Of total responses		45%	30%	25%

Table 3 Data collection methods by respondents

The use of multiple data collection methods ended up providing rather detailed accounts of the crime problems, largely owing to the complementarity of the survey, one-to-one interview and the group interview methods. The self-administer survey allowed the managers to express their opinions, views, and experiences in their own words without being influenced by the researchers' suggestions (Foddy 1993). Qualitative interviewing allowed the research team to obtain "empirical knowledge on subject's typical experiences on a topic" (Kvale and Brinkmann 2009). The group interview enabled the research team to interview multiple individuals simultaneously in a social context (Frey and Fontana, 1991). The technique allowed interviewees to reflect their own perceptions vis-à-vis the views of others, and owing to the group dynamics, group interviews may stimulate deeper and more spontaneous elaboration and expression of experiences among participants than other less interactive means of data collection (Morgan, 1996). An experienced moderator facilitated the both sessions, and two assisting co-researchers documented the sessions by taking written notes. The members of the research team documented the interview sessions by taking brief notes during the sessions and extending the notes soon after the interviews.

PART I – Crime and security problems

To which crime types is your supply chain most vulnerable?

Where do you see the most worrying trends to be regarding crime in the future?

Can you identify the top three future crime problems – and views on future security measures designed to counter or combat them?

Probing questions

Can you share an example?

Can you elaborate?

Do you have anything to add?

Box 2 Interview and survey questions in the supply chain crime taxonomy study[18]

Once the data collection was completed, I was given the task of data analysis. For this exercise, I employed the so-called content analysis technique that is particularly useful to "make replicable and valid inferences from texts […] to the context of their use" (Krippendorf 2004). As the result of the analysis process, that involved row-by-row examination of transcribed research data, I identified a set of general crime problems. The findings were discussed among the research team until agreement was reached about the nature and working definitions of the crime problems. In more technical terms, the research team arrived in the intersubjective agreement on the message contents through "discoursive alignment of interpretations" (Krippendorf 2004). Prior experiences of the research team and a handful of literature sources contributed to the refinement of the definitions of the crime problems.

The taxonomy development process took place in late 2012, and it involved mainly my two colleagues, Dr. Juha Hintsa and Dr. Luca Urciuoli, and me. In the taxonomy development process, we paid close attention to guidance in the literature. We found that a well-crafted taxonomy[19] comprise mutually exclusive classes, so that each object of classification falls into one taxonomic class only (Bailey 1994). Moreover, a taxonomy should group objects by relevant properties that form practically meaningful classes. Much of the modern chemistry, for example, is built around a useful classification, namely the Dmitri Mendeleev's periodic table that arranges elements by their atomic mass and electronic configuration and this way identifies noble gases, halogens, and other groups of elements that share similar important chemical properties. Eppler et al. (2011) propose that relevance of a taxonomy is a function of five

[18] Data collection took place as part of the LOGSEC project that had a larger scope than the taxonomy study. Therefore, researchers have been asking the interviewees also additional questions, which did not relate to the development of the supply chain crime taxonomy.

[19] According to Bailey (1994), a classification refers either to a process of grouping objects by similarity or the resulting classification scheme. Taxonomies and typologies are the two main varieties of the classifications schemes. Although many use the terms taxonomy and typology interchangeably, Bailey (1994) argues, that taxonomies are grounded in empirical data while typologies are purely conceptual. Accordingly, the classification scheme in this dissertation is a taxonomy because it is crafted on the basis of interview and survey data.

qualities: simplicity, visual clarity, usefulness, typicality, and unambiguous labeling. Simple and clear appearance of a classification scheme enables people to understand and memorize the taxonomy and facilitates its application to practical problems. The usefulness determines the extent to which the taxonomy facilitates managerial problem solving. The typicality is the degree to which objects of classification are grouped by their properties that are familiar for the managers. The unambiguous labels criterion concerns distinct and self-explanatory names of the taxonomic classes.

The literature guidance played a crucial role in the development of the supply chain crime taxonomy. My decision was to use the Problem Solving Policing framework, an approach for designing crime prevention measures through an elaborate diagnosis of crime problems, to identify meaningful properties of the supply chain crime problems. Literature on the Problem Solving Policing suggests that crime analysis can reveal key properties of any crime problem by answering to six diagnostic questions (Poyner 1986; in Clarke and Eck 2000):

- What is the criminal act? (Act)
- Where does the criminal act take place? (Setting)
- When does criminal act occur? (Timing)
- Who are involved in the criminal act? (Offenders and victims)
- Why those, who are involved in the criminal act, are involved? (Motive)
- How does the criminal act occur? (Method)

Because "What is the criminal act?" was the only one of the six diagnostic questions that could be answered on the basis of the managers' descriptions supply chain crime problems, I selected the criminal act to be the basis for the taxonomic classification. The managerial descriptions, indeed, allow us to distinguish what offenders *do* when they commit a criminal act: in cargo theft criminals take goods out of the supply chain; and in sabotage, they damage people, assets, or infrastructure. On the contrary, it is impossible to confine most crime problems into any particular setting, time, offender class, motive, or method. Cargo thieves, for example, may target cargo in transit or in warehouse (setting) during day or at night (timing). Moreover, individual cargo thieves differ in terms age, gender, educational background, or social class (offender). Furthermore, most of the cargo thieves steal apparently for financial reasons, but some cargo thieves are evidently driven by reasons such as excitement, peer recognition, or mental illness (motive). Lastly, the cargo thieves use numerous methods (or modi operandi) to get access to valuable cargo that involve varying degree of deception, violence, planning, and technical sophistication. By focusing on what the criminals are doing allowed us to reduce the complexity of supply chain crime problems into four taxonomic classes. More precisely, the taxonomic classes build on the observation that the criminals interact with the supply chain: 1) by taking assets out of the supply chain, 2) by introducing contraband into the supply chain, and 3) by attacking supply chains directly. Besides the main ways of interaction, criminals and

terrorists commonly employ a range of facilitating techniques to support their main criminal activities.

Once the taxonomy was ready, I assessed the validity of the taxonomy by applying it to the context of the Swiss-centric international postal logistics. Specifically, I mapped postal crime problems against the taxonomic classes. After this mapping exercise I consulted a Swiss Post's security manager to see whether he agrees with my interpretation. He agreed and did not suggest any modifications.

2.3.2. Systematic Literature Review

In the second research phase, I conducted a systematic literature review. I selected to delimit the review only to peer-reviewed academic studies because the extant body of academic SCS research seemed to be large enough to allow a literature synthesis to be conducted, and because only rigorous, quality research should pass through the peer-review process. Due to the focus on the peer-reviewed academic research, a large corpus of practitioners' reports, non-published studies, books, and dissertations was left out of the scope of this systematic literature review.

The first step in the location of studies was to generate key words and queries for electronic searches in academic citation databases. For this purpose, I referred to a precursory scoping study (Männistö 2011), studied closely earlier literature reviews on supply chain security (Williams et al. 2008; Voss et al. 2009a), and consulted two colleagues having extensive backgrounds in supply chain security research. Next, I arranged the key words into search queries and ran trial searches before conducting six actual queries at two major repositories of academic studies: Elsevier's Scopus and Thomson Reuter's Web of Knowledge. The Scopus catalogues contents of around 18500 peer-reviewed journals worldwide while the Web of Knowledge, or technically the Web of Science that is embedded in the Web of Knowledge, contains citation data for around 12000 "top tier" academic journals. To minimize the risk that key academic contributions would have escaped the initial searches, I searched for additional articles at the archives of six prominent logistics journals: *Management Science, Operations Research, Journal of Operations Management, Journal of Business Logistics, Journal Supply Chain Management, and International Journal of Physical Distribution and Logistics Management.* This final search was conducted in the Web of Knowledge and restricted to include only studies published in 2001 or later because the year 2001 is considered to the starting point for modern academic SCS research (Hintsa 2011). Altogether, the eight searches I conducted identified 634 candidate articles. Table 4 summaries the searches protocol in terms the applied query, used search engine, and the number of the identified articles.

Query	Search	Hits

	engine	
Secur* AND logistics OR transport* OR distribution OR cargo OR "supply chain" AND inspect* OR scan* OR vulnerab* OR program OR initiative OR risk AND theft OR smuggling OR trafficking OR contraband OR terrori* AND NOT marketing OR health OR "social security"	Scopus	105
	Web of Knowledge	205
"Supply chain security"	Scopus	34
	Web of Knowledge	25
	Emerald	57
"Supply chain" AND crime OR criminal	Scopus	27
	Web of Knowledge	15
Security (timespan = 2001-2013), only six leading journals publishing research on logistics and supply chain management	Web of Knowledge	166
	TOTAL	**634**

Table 4 Search queries and results

Next, the 634 located studies were subjected to a four-phase screening process. First, I removed 90 duplicate studies. Second, I discarded articles, which titles referred to non-related topics (e.g. passenger transport) or highly technical topics (e.g. neutron screening system). Third, I examined abstracts of the remaining 101 articles and rejected studies mainly because of the non-related topics and non-scientific abstracts. At the final fourth stage, I read through the 71 remaining articles and assessed their eligibility to the final review sample against two criteria: the relevance to the review question and quality of research design. The relevance was appraised on the basis of empirical evidence and theoretical reasoning. An article was disqualified if it scored "inadequate" in either criteria or "borderline" in both criteria (see Table 5). In total 41 articles were qualified into the final review sample.

Criterion	Inadequate	Borderline	Good
Relevance to review question	Study does not help answer the review question	Study provides some theoretical or empirical insight that helps answer the review question	Study provides substantial theoretical or empirical insight that help answer the review question
Quality of research	Description of method is opaque or insufficient; no	Description of method is somewhat clear; use of some	Method is clearly described; research is

design	use of literature or theory; poor data / unrealistic assumptions	literature and theory; scarce data / somewhat realistic assumptions	rooted strongly in literature and theory; rich data / realistic assumptions

Table 5 Criteria for appraising eligibility of candidate review articles

After concluding the final review sample of 41 articles, I extracted relevant data from each article by filling in data fields in the data extraction form (see Table 6). The data extraction form was designed to capture general information about the paper, its research context, security solutions it considers, and outcomes the paper studies. The data extraction forms of the 41 reviewed papers are presented in the Annex B.

Category	Data field (description / categories)
Overview	Problem statement (What problem does the research address?)
	Objective of the study (What does the study aim to achieve?)
	Type of paper (analytical, empirical, review)
	Strategy of inquiry and methods
Context	Settings (industry sector, mode of transport, geographical scope etc.)
	Focal crime risk (e.g., theft, smuggling, or terrorism)
Intervention	What security solutions are studied?
Mechanism	What contextual factors activate the solution-outcome association?
	What contextual factors influence the solution-outcome association?
Outcome	What are observed / assumed effects of security solutions?

Table 6 Data extraction template

Once I had extracted relevant data from the reviewed articles, I synthetized this information using a so-called "synthesis through explanation" technique. This explanatory approach to the research synthesis, as Rousseau et al. (2008) explain, is suitable for theory generation, and it can make use of diverse evidence (both qualitative and qualitative data as well as theoretical arguments). Most importantly, the synthesis by explanation aims to understand "why and where interventions lead to outcomes," which is the precise goal of the systematic literature review of this thesis. It should be noted that the explanatory approach to the synthesis is distinct from quantitative meta-analyses that aggregate quantitative evidence for higher statistical power and stronger evidence. The meta-analysis, though popular in medicine and other disciplines, lends itself poorly to the academic management research that is characterized by a plurality of research questions, methods, and theoretical perspectives (Tranfield et al. 2003).

2.3.2. Case study

The purpose of the case study research was to describe modern postal security management practices in the international postal network. Therefore, following a theoretical sampling strategy (Yin 2009), I selected the case study among the top performers of the 192 member countries of the Universal Postal Union. In the end, Switzerland was selected to be the focal country for the following reasons. The Swiss postal service is one of the most reliable services in Europe (Eurostat 2014; Swiss Post 2010), and the international trading community has ranked Swiss border formalities among the world's "trade-friendliest" in terms of speed, simplicity, and predictability of customs procedures (World Bank 2012). Moreover, owing to the advanced infrastructure (ITU 2009) and low-corruption (Transparency International 2012), the Swiss context for international logistics apparently enables implementation of the most up-to-date technologies and procedures for controlling the crime risks in the postal network. Other countries including Norway, Germany, and Finland share the same qualities with Switzerland, and these countries could have made equally suitable cases than Switzerland (see comparison of Switzerland vis-à-vis other European countries in Figure 1). Annex A provides further details). However, Switzerland was ultimately selected because of the established and trusted relationship between Swiss Post and my academic affiliation, the Chair of Management of Network Industries (MIR) of the EFPL University. This relationship enabled an in-depth investigation on this security sensitive research area. Case study methodologists Yin (2009) and Eisenhardt (1989) advise researchers to carry out multiple case studies to remedy the problem of generalizability. Two reasons, however, led me to disregard this piece of advice. First, as the case study aimed at deep contextual understanding, I decided to expend my time on single in-depth study rather than on multiple less profound case studies. Second, the established relationship with Swiss Post and my academic affiliation, enabled me enter a unique research setting, which had been previously inaccessible to scientific inquiries. As I had this privileged access only in Switzerland, it would have been difficult to conduct equally profound replicative case studies elsewhere.

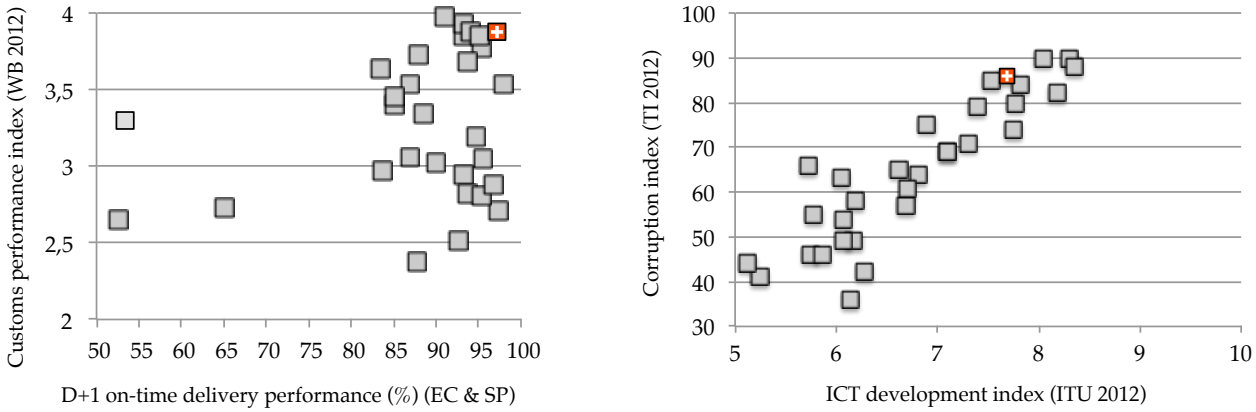


Figure 1 Comparisons used in case country selection

The frame for the case study was outlined based on information collected through scoping interviews with three postal managers, two customs experts, and two academics. The interviews were unstructured, casual conversations about crime and security risks in the postal network. The scoping interviews guided the subsequent data collection, data analysis, and the case study composition.

The data collection followed the Yin's (2009) three principles: use of multiple sources of evidence, establishment of case study database, and ensuring a chain of evidence. I tapped into multiple sources of evidence, in particular interviews, documents, and field observations, to gather rich data from multiple sources. This allowed me to triangulate data sources, that is, to crosscheck whether multiple sources of information support facts and emerging interpretations (Patton 2002). So, in the midst of the analysis and the case composition, I could resume data collection and collect additional evidence in order to test and refute emerging concepts, hypotheses, and conclusions. The case study database was established at the outset of the research, and this database was the place where I deposited all case study evidence I managed to collect. The database – a meticulous archive of the audiotapes, transcripts, field notes, and memos – made it possible to connect interpretations and conclusions to the supporting (raw) case study evidence.

Over course of the case study research, I collected inputs from numerous individuals. Their titles and affiliations are presented in the Table 7 below. It is important to note that one Swiss Post's security manager played a key role in the data collection by participating in five one-to-one and three group interview session, sharing critical documents, and validating most facts and interpretations of the case study descriptions. Moreover, he introduced me to other relevant informants within the Swiss Post organization and the Cantonal police. I also consulted two advisors, Prof. Matthias Finger and Dr. Juha Hintsa, to identify and contact experts in suitable government agencies and international organizations.

Organization	Title	Type of interview
Swiss Post	Security Manager	One-to-one (× 5) / group†^π
	Import manager	Group†
	Mail handling manager	Groupπ
International Post Corporation	Supply chain integration specialist	Group
World Customs Organization	Technical Officer 1	One-to-one / group★
	Technical Officer 2	Group★
Swiss Customs	Supply Chain Security expert	Group″
	Customs procedure expert	Group″
	Risk assessment expert	Group″
INTERPOL	Senior Crime Analyst	One-to-one
	Counter-terrorism Expert	One-to-one
Swiss Cantonal Police	Commissaire Principal	Group^
SWISS WorldCargo	Process engineer	One-to-one

Table 7 Case study interviews

Semi-structured one-to-one and group interviews were the main data collection methods in the case study research. The semi-structured interviews were guided by an interview protocol that outlined main themes, questions, and formalities (e.g., introductions, promise of confidentiality, follow-up collaboration). In general, the semi-structured approach allows the interviewer to divert from the prescribed mix, sequence, and wording of questions to keep the conversation casual and allow spontaneous discussion on emerging interesting topics (Kvale and Brinkman 2009). The use of interview guide increases the depth of data, systematizes data collection, and enables the investigators to anticipate and fill logical gaps in the respondent's narrative (Patton 2002). Box 3 outlines the questions of the interview protocol. This general protocol was adapted for each interview session, mostly by adding technical questions and omitting irrelevant ones. The interviewees received their tailored interview questions some days prior to the interview sessions. The sessions lasted between 30 – 180 minutes. The interviews were audiotaped and afterwards transcribed to a reasonable detail. Lastly, if deemed necessary, I sent the interview findings back to the interviewees for validation.

PART I – Crime and security risks

How significant problem is risk X to your organization?

PART II – Crime and security risk controls

How do you control risk X?

How, when, where, and why do you carry out control Y?

What percentage of traffic Z is subject to control Y?

What role does information play in controlling risk X?

What do you do when you encounter risk X?

PART III – Collaboration and information exchange

Which parties do influence your decisions on risk control priorities and strategies?

How do you interact with other organizations when controlling risk X?

What information do you receive / share from other organization?

How, when, and why do your receive / share data?

Probing questions

Can you share an example?

Can you elaborate?

Do you have anything to add?

Box 3 Questions of the general case study interview protocol

Besides interviewing, I collected case study data by tapping into publicly available sources of contextual information, reviewing relevant regulations and Swiss Post's internal documents, and conducting on-site observations. The publicly available data sources included online statistical databases (e.g., Eurostat), reports (e.g., UPU's document repositories), and news archives (e.g., BBC). This contextual data helped me to frame the context of the case research and crosscheck interview findings. Laws and regulations are a source of important contextual information that set the de jure basis for the postal service domestically and abroad. Therefore, I conducted legal reviews on 1) supply chain security and 2) civil aviation security. I also analyzed relevant companies' internal documents I managed to get in my hands.

Lastly, to deepen the my understanding on the mail handling processes, I did field trips to one of Swiss Post's airmail exchange office and on of the parcel sorting centers. In both trips, I was accompanied by a senior manager who in charge of the postal facility and who guided me through the process and demonstrated normal procedures and emergency routines. The field trips produced descriptive and reflective notes, sketches, and photographs outlining the sequences of procedures postal items undergo as they flow through the handling process. The two around 60 minute field trips were followed by a debriefing session during which I had opportunity to ask further questions.

The first steps of the data analysis included cleaning the interview transcripts and field notes from irrelevant text passages, writing reflective text around verbatim quotes and observations, and clustering connected passages together within a single document. To minimize the risk of loss and distortion of information over the data cleaning and analysis process, I crosschecked facts and emerging interpretations by comparing the cleaned interview documents, raw

transcripts, and the audiotapes. I read through the case material and searched for data segments that represented activities, actors, and other constructs I had outlined in the a priori conceptual framework. Throughout the analysis, I refined the a priori framework as new conceptual categories surfaced from the research data. As the coding progressed, certain categories collapsed into more abstract theoretical classes (e.g. urgency of controls) while some categories turned out to be irrelevant. As Miles and Huberman (1994) suggest, I switched recursively between the data collection and the data analysis activities. This back and forth process gave me flexibility to revise the interview questions and interview new informants to collect additional data on unexpected, emergent concepts (e.g., controlled delivery). Especially, the findings of the first analysis round strongly influenced the subsequent data collection. I modified or discarded the emergent conceptual categories, if subsequent interviews, document analysis, or on-site visits revealed conflicting evidence. The second read-through of the case study material revealed more nuanced properties of and differences across the conceptual categories, which enabled me to start collating case study evidence into data displays and start drafting the case study report. Over the course of the third analysis round, the refinements to conceptual categories became increasingly incremental, and the list of conceptual categories seemed to stabilize. During the data collect and analysis, I constantly attempted to refute emerging interpretations and findings through an active search of conflicting evidence. Knowledge claims that survive such falsification attempts have high credibility. To conclude this section, Table 8 below summaries research methods by each of the three studies – the supply chain crime taxonomy, the systematic literature review, and the case study – that comprise the core research contents of this dissertation.

	Preparation		Data collection				
	Literature review	Scoping interviews	One-to-one interviews	Group interviews	Document review	On-site observation	Survey
Taxonomy	X	X	X	X			X
SLR	X	X			X		
Case	X	X	X	X	X	X	

	Data analysis	Validation	
	Content analysis	Expert interviews	Case study

Taxonomy	X	X	X
SLR	X	X	
Case	X	X	

Table 8 Methods by research phase and study

2.4. Research quality

Four established quality criteria for positivistic/quantitative research – internal validity, external validity, reliability, and objectivity – have their counterparts in the qualitative research tradition (Lincoln 1989). The equivalent of the internal validity in the qualitative realm is credibility, a measure for assessing the degree of match between an interviewee's notions and the researcher's reconstruction of these notions. While the external validity relies strongly on statistical inferences on generalizability of findings beyond the study's population, transferability assesses more qualitatively the extent to which evidence allows the researcher to state general claims about the reality. Qualitative research is rarely replicable in the positivistic sense due to the evolving research context and flexible data collection and analysis techniques. Therefore, instead of positivistic reliability, qualitative research aims at high dependability – the degree, to which others are able to trace but not necessary replicate the logic and the process of the research. Most social scientists acknowledge that objectivity is an elusive ideal as all research and knowledge is more or less biased by subjectivity. Thus, qualitative researchers pursue confirmability through systematic reduction of the subjective bias and through elaboration of logic and procedures followed to refine research data into conclusions and recommendations. Building on Lincoln (1989), Erlandson et al. (1993) propose that the four quality criteria for qualitative research – credibility, transferability, dependability, and confirmability – determine the trustworthiness of a qualitative research product. Table 9 defines the four quality criteria and lists safeguards I have taken to protect credibility, transferability, dependability, and confirmability of this PhD research.

Determinant of trustworthiness	Strength (+) and weakness (-)	Taxonomy	Case	SLR
Credibility				
"Degree of match between the respondent's constructions and researcher's representation of these"	Follow-up communications with respondents as needed	+	+	N/A
	Triangulation of data	+	+	N/A

	sources			
	Audio recording of interviews	-	+	N/A
	Refutation attempts of initial conclusions	+	+	+
Transferability "Extent to which the study is able to make general claims about the world"	Theory-driven sampling	+	+	N/A
	Analysis of similarities and differences between the sending and possible receiving contexts	N/A	+	N/A
Dependability "Extent to which changes in research design are traceable"	Adherence to a formal research protocol	+	+	+
	Reporting changes in research design	+	+	+
Confirmability "Extent to which conclusions, interpretations and recommendations can be traced back to and substantiated by data; degree of freedom from researcher's bias"	Storage of research data in an online database	+	+	+
	Content analysis by single (-) / multiple (+) coders	+	-	-
	Use of experienced moderators in group interviews	+	N/A	N/A
	Fields in data extraction form correspond cells in data display tables	N/A	N/A	+

Table 9 Appraisal of research quality

2.5. Ethical and data sensitivity considerations

There is always a risk that people abuse research findings for illegal or unethical purposes. The risk of abuse is particularly high in security research like this PhD project. This is because criminals and terrorists tend to be calculating antagonists (Ekwall 2009a) who adapt their behavior in response to information on risks and rewards of crime opportunities (Cornish and Clarke 1987). Recognizing the risk of criminal abuse, I have taken some precautionary measures. To make sure that this thesis document does not contain any confidential or security-sensitive information, my key informants have reviewed the contents of this dissertation. Thus, all facts presented on the pages of this dissertation are either publicly available information or have been accepted for unrestricted publication by the informants. Nevertheless, I acknowledge that certain observations, statements, and interpretations that arise from the synthesis of

multiple pieces of information might indeed entice or facilitate crime and terrorism. Therefore, I have purposefully kept some parts of the discussion at a general level, even if the depth of my research would have allowed more detailed elaboration. Most importantly, this thesis document does not discuss covert security controls that might exist but are known only to law enforcement or security specialists. Altogether, this research may increase common awareness of security management in the postal logistics networks, and this heightened consciousness could, in fact, discourage potential smuggles, mail bombers, and thieves from attempting crime.

I have followed another set of safeguards to protect people who have provided data inputs to this research or otherwise helped me to pursue this research. Whenever I interacted with potential or the actual informants, I was transparent about my intent, affiliation, and sponsors. I offered all informants pseudonymity, but many of them allowed me to report their real names in this dissertation. A stringent data protection protocol was followed over the entire study to guard the informants' identities: each document and audiotape containing names and affiliations of the informants were stored in a secure online file hosting service, and no paper-based privacy-sensitive documents were stored.

Summary

This chapter elaborated and justified methodological choices of this doctoral research. It showed that the research is ingrained in the constructivist research philosophy that relies largely on qualitative data collection and data analysis techniques. The chapter also informed that this doctoral dissertation comprises three interconnected (and separately publishable) studies, each of which addresses a distinct research problem, uses a different dataset, and applies special research methods. The first study seeks to analyze managerial descriptions of crime problems to develop a taxonomy of supply chain crimes. The second study aims to identify and synthetize relevant academic SCS studies to extract principles of logistics-friendly SCS management and to outline an agenda for future research. The purpose of the third case study is to test the findings of the two earlier studies in practice by applying them into the case study context. The case analysis also intends to develop concepts for improving postal security management. The chapter concluded by shedding light on strengths and weaknesses of the methodological choices and detailing safeguards taken to protect informants and mitigate the risk of abuse of the research findings.

Chapter 3 | Systematic literature review

This chapter characterizes and synthesizes peer-reviewed academic studies on supply chain security (SCS) from 2001 to the present day. The analysis reveals methods, contexts, theories, and themes that define the extant body of academic SCS knowledge. The chapter studies what SCS solutions are and elaborates key dimensions of SCS performance. The review chapter also examines implications of SCS implementation to the SCS performance and logistics performance. The final part of the chapter discusses themes and principles of logistics-friendly design of SCS systems.

3.1. Post-2001 academic supply chain security research

This section characterizes the sample of 41 articles that were included in this systematic literature review. The characterization shows distribution of studies over years, presents authors who have been publishing academic studies on SCS, and introduces prominent research topics, theories, and methods the SCS discipline has fostered.

3.1.1. Overview of studies

This systematic literature review is based on the analysis of 41 systematically selected peer-reviewed academic research articles that has been published in 2001 or later. This sample of studies, as Figure 2 shows, has been published rather unevenly over years. Although the first study dates back to year 2003, as many as 88% (36) of the studies have been published in 2008 or later. The fact that the most SCS articles are no older than six years partly explains why earlier literature reviews on SCS (Voss et al. 2009a; Williams et al. 2008) have considered mainly studies on general supply chain risk management rather than SCS-specific studies.

In the reviewed sample of 41 articles, empirical (17; 41%) and analytical (17; 41%) papers outnumber conceptual ones (7; 17%). Six of the empirical studies use the survey method, two articles employ the case study method, and four articles rely on interviewing as the primary research method. Other applied empirical methods include the Delphi paneling, expert group interviewing, and the analysis of operational logistics data. The review sample includes five multi-method studies that employ more than one data collection techniques. The analytical studies rely predominantly on the queuing network analysis, game-theoretical modeling, and

the multi-criteria decision analysis. All literature review papers are narrative traditional analyses, that unlike this review, do not follow a systematic and transparent review protocol.

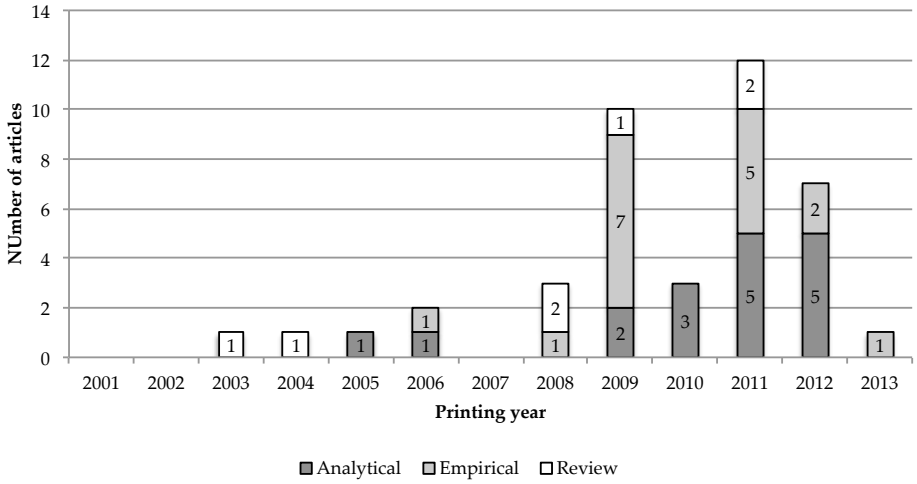


Figure 2 Number and type of studies over years

The reviewed academic studies have been published in 24 scholarly journals. The five most important publication outlets and the primary forums for the academic SCS debate have been the *International Journal of Physical Distribution and Logistics Management* (4, 10%), *Annals of Operations Research* (3, 7 %), *International Journal of Logistics Management* (3, 7%), *Journal of Business Logistics* (3, 7%), and *Risk Analysis* (3, 7%). In general, the previous SCS research has been largely interdisciplinary. Rather unexpectedly, only around half of the reviewed articles have been published in management journals. The other half has appeared mainly in social policy, engineering, and computer science journals. Overall, looking at the list of journals that have published SCS research, scholars should no longer worry whether the SCS research is too marginal for top-rank generalist "big tent" journals that boast high impact factors. That is simply not true: *Management Science,* and *European Journal on Operational Research,* among other leading operations management journals, have published studies on SCS.

Regarding the authorship, 83 individuals have contributed to at least one of the 41 reviewed articles. Of these authors, 55 (66%) were affiliated with US-based organizations at the time they submitted their articles. The rest of the authors were based in the UK (5, 10%), Belgium (5, 6%), Sweden (5, 6%), Switzerland (5, 6%), Taiwan (2, 2%), China (1, 1 %), Republic of Korea (1, 1%) and Turkey (1, 1%). Only five articles (12%) have been written in international research teams, which strikes as a surprise given the global nature of the SCS management practice.

3.1.2. Research themes

Maritime SCS studies stand out as the most prominent theme in the literature. Centering on inspection strategies for detecting illicit radiological and nuclear material in shipping containers, the maritime literature offers mainly normative guidance how to optimize container screening systems (e.g., Wein et al. 2006; Merrick and McLay 2010; Bakir 2011) and how to integrate SCS solutions into port logistics processes (e.g., Sternberg et al. 2012; Belzer and Swan 2011; Bakshi et al. 2011). As the exception to the port-centric maritime literature, Roach (2004) offers a shrewd legal analysis on legal barriers that prevent law enforcement from pursuing crime and terrorism at the international waters. Another prominent research themes is road transportation security: Klima (2012) discusses factors that make trucking vulnerable to security risks, Haelterman et al. (2011) debate costs and benefits of preventive security solutions in the express courier context, and Ekwall (2009b) studies effects of in-transit and facility security on cargo thieves' behavior. Rather surprisingly, the SCS research has neglected some key modes of transport. None of the studies, for instance, addresses air cargo security, and only one discusses rail transport (Reilly et al. 2012). There are a few papers in the reviewed sample that focus on a specific industry sector. Voss et al. (2009a) discuss the impact of security implementation on the security performance in the food industry, and Joossens and Raw (2008) study smuggling of cigarettes into the UK, by focusing on the tobacco industry.

Most of the reviewed studies consider SCS from the viewpoint of (private) economic supply chain operators, including shippers, carriers, freight forwarders, and port operators. It appears, however, that this emphasis on the economic operators has come at the expense of other views. Despite the central role of governmental agencies in the SCS practice, except for few studies (e.g., Bakshi et al. 2011), the past research has largely overlooked their perspective. Another neglected perspective is the one of criminals, the antagonists responsible for crime and terrorism in the global supply chain. The antagonist view is discussed in some game theoretical studies, but only analytically without empirical data and assuming rather unrealistically the rationality of the criminals (e.g., Bakir 2011; Bakshi and Gans 2010). Another major theme, trade facilitation literature (e.g., Signoret 2009; Hameri and Hintsa 2009; Grainger 2011) takes a broad perspective and debates past and future implications of SCS implementation on the global trade.

The SCS literature concentrates on certain supply chain crime phenomena more than others. The counter-terrorism, no doubt an important crime theme, permeates through the entire literature, and it is particularly prominent in the maritime, trade facilitation, and critical infrastructure studies. The thematic bias toward terrorism is reasonable given that many articles are written in the US from the "homeland security" perspective, which involves a strong counter-terrorism focus. However, it strikes how much the US research differs from the

continental European research in terms of the crime focus. While the US-based scholars deal invariably with the threat of terrorism, their European colleagues dedicate their attention to more conventional supply chain crime threats such as cargo theft (Ekwall 2009b), trafficking in counterfeits (Staake et al. 2009) and smuggling in illegal cigarettes (Joossens and Raw 2008).

The extant SCS literature fosters many theoretical perspectives. Game theory is widely used in analytical papers to assess effects of SCS solutions on criminal reasoning and behavior. Empirical, data-driven studies aim to understand the criminal behavior mainly with criminological theories, of which the theory of situational crime prevention (Haelterman et al. 2012; Speier et al. 2011) and the theory of crime displacement (Ekwall 2009b) have been particularly popular in the SCS literature. Articles studying the impact of SCS implementation on operational performance rest mainly on the principles of the queuing network analysis (Bakshi et al. 2011), the total quality management (Lee and Whang 2005; Sheu et al. 2006), the game theoretical modeling (Bakshi and Gans 2010), and on the general theory of supply chain integration (Williams et al. 2008).

Academics have developed many tools to help managers select a suitable mix of security solutions among a broad variety of alternatives. Building on his previous studies, Haelterman and his colleagues (2012) demonstrate a conceptual framework for selecting preventive SCS measures to counter theft (to some extent terrorism and smuggling). Approaching the problem from the criminological angle, Haelterman et al. (2012) identify and measure significance of a set of preconditions, various cost elements, and possible reverse effects that managers should be aware of prior implementing any preventive SCS strategies. Assuming a more quantitative approach, Urciuoli (2011) develop an analytical method for assessing cost-effectiveness of anti-theft solutions. Quite similarly, Talas and Menachof (2009) apply the classic portfolio theory (famous in finance) to come up with a method for allocating security budget optimally across sixteen SCS solutions in a seaport environment[20]. Acknowledging that reliable numerical data on performance metrics of a single security solution is very hard to obtain, Yang et al. (2009) apply fuzzy logic reasoning to bridge the gap between the quantitative and the qualitative SCS management models. Their fuzzy logic tool translates subjective and qualitative managerial judgements into numerical form, which allows rough estimation of expected security benefits and costs. Game theoretical studies on container inspection discuss trade-offs of various combinations of the inspection technologies, procedures, and policies, thus providing normative guidance for policy making. Bakir (2011) develops a model to analyze ways to allocate security budget across physical security solutions, container monitoring sensor technology, and non-intrusive inspection methods (mainly variants of X-ray imaging

[20] The model of Talas and Menachof (2009), for example, require accurate estimates on "performance" of SCS solutions (both for the mean performance and that standard variation of the performance).

techniques) in domestic and foreign seaports. Wein et al. (2006) restrict their analysis to eleven complementary solutions, namely "shipper certification, container seals, and a targeting software system, followed by passive (neutron and gamma), active (gamma radiography), and manual testing at overseas and domestic ports."

To conclude so far, the literature synthesis reveals that SCS has attracted cross-disciplinary and steadily growing academic interest since 2001. The discipline has undergone a shift from conceptual studies towards empirical and analytical research. For the most part, the SCS research has produced management tools and normative guidance for policy makers. Dominant themes in the literature include trade-offs involved in shipping container screening, protection of cargo from theft and tampering, and systematic selection of SCS solutions among multiple options.

3.2. Supply chain security management

This section reviews the academic SCS literature with the aim of exploring the full range of SCS solutions, identifying their essential characteristics, and examining extant academic classifications of the solutions. The second part of the section shifts attention to key dimensions of the SCS performance.

3.2.1. Diversity of supply chain security solutions

In this thesis, the term security solution is used to talk about means to mitigate supply chain security risks (likelihood and/or impact). The notion of security solution is synonymous with a variety of terms the SCS academic literature uses: security measures (Haelterman et al. 2012; Hameri and Hintsa 2009; Ekwall 2009b), security investment options (Yang et al. 2009), resource allocation strategies (Bakir 2011), principles (Lee and Wolfe 2005), and layers of protection (Wein et al. 2006), security solutions (Urciuoli 2009), and security management attributes (Yang and Wei 2013).

As the diversity of the terminology implies, the academic literature discusses a broad range of supply chain security (SCS) solutions. Many of the solutions involve a technological component. Burglar alarms, CC-TV camera systems, and electronic key cards are examples of technology-centric facility protection solutions. Outside the four walls logistics facilities, when cargo travels aboard ships, trucks, and other modes of transport, many logistics operators use RFID tags, GPS trackers, and electronic container seals, and other tracking technologies to monitor their freight in transit. The tracking technologies help detect and respond swiftly to many anomalies in routing, inexplicable stops, or unauthorized openings of cargo units (Sternberg et al. 2012; Lee and Whang 2005). Security technology plays also a central role in border controls: customs administrations worldwide use increasingly automatic computer systems to risk assess

incoming / outbound traffic (Hintsa et al. 2011). If the risk assessment results indicate need for inspection, the customs authorities may apply a range of screening technologies: non-intrusive imagining techniques (e.g., X-ray, gamma ray, and neutron-based solutions), material trace detection devices, and passive radiation detectors (Wein et al. 2006).

Another key element in many SCS solutions is a set of operational procedures, or instructions that guide what managers and workers should do to fulfill their security duties. A good example of a security-related operational procedure is pre-employment background vetting, which can involve the managers calling earlier employees, the police, and credit card agencies to assess trustworthiness of prospective hires. Other examples of the operational procedures include regular training sessions, scheduling of guard patrols, and verifications of security seals, and ways security-sensitive information is shared. In the list of preventive SCS solutions, presented in Haelterman et al. (2012), awareness training, formal (security) instructions, compliance checks, double drivers, and over security escorts count as the operational procedures.

Many security solutions seem to be incremental adjustments to the already existing security systems. For instance, a great deal of the maritime SCS research discusses how seemingly small adjustments of alarm thresholds or re-arrangements of screening technologies affect security and speed of port logistics (McClay and Dreiding 2012; Wein et al. 2006; Bakir 2011). Quite the same way, IT-based SCS solutions, that are said to increase security and logistics performance through higher supply chain visibility (Lee et al. 2011; Sternberg et al. 2012), are incremental updates to the existing information sharing systems. The difference between the past and the modern supply chain visibility solutions is only the convenience of accessing the visibility information (e.g., status and location of shipment). I mean, a couple of decades ago, managers needed to call or fax their business partners to get information about the status of their shipments, but today the same information is often readily available in digital form. Also aiming at incremental improvement, Roach (2004) proposes updating the IMO's SUA convention[21] to enable more effective law enforcement at international waters.

It is important to notice that a single operational procedure can function as a standalone solution. However, is more common that the operational procedures are sub-components of more complex socio-technical solution systems. A classic example of a socio-technological system is a constantly monitored CC-TV system: the camera technology helps guards to detect burglars in action and catch the intruders red-handed before they manage to break in (or escape). A security system, a combination of security solutions, has been a crucial concept in theory building. In fact, none of the reviewed SCS studies investigate effects of a single practice

[21] Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) of the International Maritime Organization (IMO)

or technology in isolation. This makes sense because SCS implementation rarely starts from a clean slate, so the effects new of solutions get confounded with co-occuring effects of the existing security solutions and make it difficult to factor contributions of the single solutions out of the aggregate effect. Sheu et al. (2006) study the C-TPAT program, which comprises numerous SCS solutions. Likewise, considering aggregate effects of multiple IT-based security solutions, Sternberg et al. (2012) investigate whether SCS implementation eliminates efficiency and security problems in a seaport environment. Also survey studies, such as Martens et al. (2011) and Yang and Wei (2013), refer to single solutions (e.g., collaboration with suppliers) in their questionnaires but discuss associations between the SCS implementation and the SCS performance at the aggregate level.

Scholars and practitioners have summarized the diversity of the SCS solutions in many Conceptual frameworks. The three-by-two classification of Rice and Caniato (2003) is one of the earliest attempts to capture the diversity of the SCS solutions in a generic framework. In their view, the SCS solutions protect physical facilities, information, or freight, either at the basic level or the advanced level. The basic level security measures involve widely adopted ordinary practices, and the advanced measures involve "more forward-thinking initiatives." Alas, the arbitrary nature of this basic-advanced dichotomy becomes apparent when trying to force-fit security measures such as access control, firewalls, cargo seals, training in information security, and vulnerability testing by external experts into the basic and advanced response classes (only the two latest are "advanced" responses). In another practice-oriented classification, Rice and Spayd (2005) suggest that managers can allocate SCS investments across eleven areas where the spending may bring collateral benefits[22]. The problem with this classification is that it confuses means with goals of the SCS management and that it consists of largely overlapping categories. Can managers, for example, invest in "asset tracking and monitoring" without spending money on "proactive technology" or "transportation and conveyance security"? It is also unclear whether "personnel security" is about protecting the staff from supply chain crime, or leveraging human resources to combat the crime itself, or discouraging the staff from committing crime. The same problem of mixing up the goals and means undermines the value of the PriceWaterhouseCooper's (2011) classification, which suggests that SCS investments can be allocated across management areas of security partnerships, personnel security, ICT security, process security, and physical security.

Also academic works have classified SCS solutions by the areas of management attention. The main difference between the academic and the practitioners' works is that the academics have

[22] The eleven areas are asset visibility and tracking; personnel security; physical security; standard development; supplier selection and investment; transportation and conveyance security; building organizational infrastructure awareness and capabilities; collaboration among supply chain partners; proactive technology investments; and voluntary security compliance.

generally used more transparent and systematic methods for constructing classifications than the practice-oriented studies. Summarizing the previous literature, Autry and Bobbit (2008) come up with four general categories of the SCS solutions: a) preparation and planning initiatives, b) security-related partnerships, c) organizational adaptation, and d) security-dedicated communications and technology. Yang and Wei (2013) conduct first a literature review and expert interviews to come up with a list of maritime SCS solutions, and then they administer a survey and run an exploratory factor analysis[23] with the survey data. They find four general dimensions of the maritime SCS management: facility and cargo management, accident management and processing, information management, and partner relation management. Gutiérrez and Hintsa (2006) analyze requirements of nine voluntary SCS initiatives[24] and end up with six areas of the SCS management that require managerial attention: facility management, cargo management, human resource management, information management, business network and company management systems, and crisis management and disaster recovery. The 8-layer management model of Hintsa (2011) illustrates how fighting crime in the supply chain context involves top-level risk assessment, hands-on design and planning, implementation of a variety of technologies, procedures, and incentives as well as preparation for dealing with the consequences of supply chain crime. The model's eigth layer is particularly interesting because it suggests that companies and authorities disrupt the *criminal* supply chain, and thus influence costs, risks, and rewards of crime by disrupting supply and reducing demand of illegal goods[25]. Sarathy (2006) highlights vulnerable points in the global supply chain and suggests that SCS solutions protect goods, factories, supply chain providers and partners, freight carriers, people, or information. Reflecting the idea of the vulnerable sections in the supply chain, Urciuoli (2009) suggests that the SCS solutions could be implemented at different, hierarchical supply chain levels: while certain solutions are deployed at conveyance level (e.g., vehicles immobilization devices), other solutions may focus on smaller supply chain entities, such as cargo units and single products. A common view in the literature (Urciuoli 2009; Gutiérrez 2007; and Hintsa et al. 2010b) is to distinguish SCS solutions by the point of time they enter into effect: before crime occurs (preventive solutions), while the crime occurs (detective solutions), and after the crime has already occurred (recovery solutions).

[23] The exploratory factor analysis is technique to identify a smaller set of general concepts that summarize a group of specific concepts. For example, Yang and Wei (2013) find that 30 security management attributes (i.e., maritime SCS solutions) fall into four general categories, namely facility and cargo management, accident management and processing, information management, and partner relation management.

[24] BASC, PIP, C-TPAT, WCO SAFE, EU AEO, ISO 28000, TAPA, StairSec, and Secured Export Partnership.

[25] To disrupt supply of illegal goods the companies could employ private detectives to trace the source of the counterfeit drugs and arrange raids with local authorities as soon as rogue factories are identified. To reduce demand for illegal goods, the companies could launch a public awareness campaign about the dangers of black-market goods, such as counterfeit medicines.

To summarize so far, the literature synthesis suggests that the SCS solutions cover a broad array of technologies, procedures, and principles that allow organizations to mitigate crime risks in the supply chain. These solutions are nearly always studied and implemented as system, combinations of many solutions. The literature implies that the SCS implementation rarely starts from a clean slate: most SCS projects build on top of the existing systems, and they typically introduce incremental (though often consequential) changes to the present systems. We also found that both academics and practitioners have tried to reduce the complexity of SCS solutions into conceptual frameworks but only with modest results.

3.2.2. Supply chain security performance

There seems to be a broad consensus among supply chain risk management scholars that the goal of the SCS management is to mitigate the risk of criminal activities in the supply chain context (e.g., Closs and McGarrel 2004; Manuj and Mentzer 2008; Pfhol et al. 2010). If this is the goal, then the performance of the SCS management is determined how well the SCS solutions mitigate such crime risks. To briefly recap the forthcoming supply chain crime taxonomy chapter (Ch. 4), the SCS management addresses three main types of criminal activities. The first crime type covers *theft* and its varieties, offenses that involve unauthorized removal of assets from the supply chain. The second type, *smuggling*, encompasses crimes that involve criminals introducing contraband or security threats into the supply chain. The third *direct attack* crime type comprises instant assaults on assets, infrastructure, and people associated with the supply chain. The taxonomy clarifies the crime risks that the SCS management addresses. However, what remains unclear and disputed in the contemporary academic thinking are dimensions and indicators of the SCS performance.

The maritime SCS studies generally consider the SCS performance in terms of the ability of an inspection system to detect nuclear material or weapons in (US-bound) shipping containers. The key security performance indicator is the detection probability (aka the detection rate or the rate of true positives), which measures simply the percentage of real threats detected. Another security performance indicator in the maritime studies is the ability to deter terrorist organizations from attempting an attack (e.g., Merrick and McClay 2010; Gaukler et al. 2012; Bakir 2011; and Bakshi et al. 2011). The deterrence effect starts to apply when terrorists decide not to attack because they perceive that the risk of failure is too high due to effective inspection systems. The deterrence effect is further intensified if the terrorists perceive that there is a credible threat of forceful government retaliation against the attackers (Bier and Haphuriwath 2011).

Outside the maritime SCS literature, Belzer and Swan (2011) highlighting the key role of the human resource management in the SCS practice and point out that motivated and vigilant

employees play an important role in preventing and detecting crime and terrorism. Studying links between a seaport and hinterland logistics hubs, Sternberg et al. (2012) consider that improving ability to detect anomalies during truck transport into seaport contributes to security. Unlike in the container screening papers, the focus of Sternberg et al. (2012) is on detecting situations when cargo integrity is about to break rather than on detecting undeclared content inside the containers, which integrity has already been broken at the origin or at some point in the supply chain. Some scholars have also emphasized contribution of the SCS implementation in assuring supply chain continuity (Autry and Bobbit 2008) or reducing the likelihood or duration of possible supply chain disruptions (Murray-Tuite and Fei 2010; Bakshi and Gans 2010).

Taking a broader look across modes of transport, Gutiérrez (2007) summarizes that basic objectives of the SCS management are prevention, monitoring & detection, and reaction to an anomaly or a failure[26]. In the empirical literature, Voss et al. (2009a) adopt this idea to an extent and measure the SCS performance in terms of the frequency of security incidents, the ability to detect the incidents, and the capability of recovering from the incidents. Hintsa et al. (2010b) and Urciuoli (2009) offer a slightly different interpretation of the "phases" of the SCS management by arguing that the SCS solutions either prevent, detect, or help recover from security breaches. Anyhow, some of these concepts are rather ambiguous. Gutiérrez (2007) considers prevention in terms of discouraging criminals from attempting crime, but this is not the view of Hintsa et al. (2010b) and Urciuoli (2009) who consider prevention not only as a way deter criminals from committing crime but also as way to prevent security crimes when criminals have already decided to commit and discouragement is no longer relevant. In other words, their view on the crime prevention is more about preventing breaches of the supply chain integrity rather than discouraging crime attempts altogether. The interpretation of Haelterman et al. (2012) muddies the waters further. They consider key cards, alarms, GPS tracking, and use of double drivers as preventive measures. It is clear that many of these solutions have as much do with criminal investigations as the crime prevention. In fact, in the view of Haelterman et al. (2012) the attribute "preventive" refers to the fact the SCS solutions are implemented ex-ante, before crime occurs and not as corrective / investigative measure after occurrence of the crime. The attribute of preventive can be therefore seen synonymous with proactive.

The literature contains more or less biased operationalizations of the SCS performance. The academic studies have used mainly perceptional measures to gauge the SCS performance

[26] In her view, prevention is about discouraging criminals from attempting crime, monitoring & detection about getting informed about ongoing suspicious activities, and anomaly reaction a way to resolve problems and get the supply chain back to the normal state.

mainly due to lack of reliable statistical data (e.g., Voss et al. 2009a; Yang and Wei 2013; Speier et al. 2011; Martens et al. 2011). Sternberg et al. (2012) avoid the problem of measuring altogether by observing whether security and efficiency problems disappeared after the implementation of a set of IT-enabled efficiency solutions. Lee et al. (2011) consider the SCS performance rather narrowly as the organization's ability to locate and eliminate the source of a product contamination. Their measure focuses on the recovery dimension of risk management: measures taken after an undesired risk event has already occurred. Another issue with operationalization of Lee et al. (2011) is that they make no difference between safety and security risks: they talk about security but refer to unintentional quality control problems. This reference to involuntary occurrences is wrong if we stick to the definition of security risks as something caused by deliberate criminal activities. Falling into the same trap of mistaking security for safety, Yang and Wei (2013) define SCS performance in terms of (work) safety and customs performance. As most accidents occur due to negligence, equipment failure, and poor management, the work safety is a biased measure for the SCS performance. The second proxy Yang and Wei (2013) use, the customs performance, is no less biased measure as the work safety because the customs performance (measured as waiting time at border and frequency of inspections in the paper) is affected by many other more consequential factors than the security performance, for example the prevailing risk landscape and competency of customs brokering staff.

To sum up this sub-section, many academic SCS thinkers seem to agree that the SCS performance is about preventing, detecting, and recovering from crime. However, there is still some confusion about the nature of the SCS performance. Some academics mistake security risks for safety risks, define the SCS performance unnecessary narrowly, or use biased proxy measures to estimate the SCS performance.

3.2.3. New supply chain security performance model

The literature synthesis offers a new perspective on the SCS performance that allows us to come up with a new comprehensive model for the SCS performance. The basis of the novel model is the idea that supply chain crime can be understood as a four-phase process, which is divided by three decisive moments: 1) the decision to commit crime, 2) breach of the supply chain integrity, and 3) the escalation of a crime incident. In the first phase, potential criminals prepare for crime by identifying crime opportunities and by weighing perceived risks and costs of these opportunities against expected rewards. If the prospective rewards outweigh the estimated risks and costs, under the assumption of the bounded rationality, the criminals decide to commit crime. One of the goals of the SCS solutions is thus to discourage crime through reduction of rewarding crime opportunities. More or less contextual techniques for reducing the crime reward include tagging property with distinctive marks, knitting brand logs into

garments only after a risky shipping passage, denying publicity from terrorist attacks, locking electronic devices with activation codes, or shipping left shoes in one consignment and right shoes in another. Ways to increase perceived risks and costs of crime include display of active law enforcement (e.g., police or guard patrols), boasting of successful seizures and arrests, and rumor spreading about effective covert security defenses. Methods for reducing the crime opportunities include removal of indicators of high value (e.g., logos or distinctive colors of a high-tech company) and parking trucks and trailers only at secure parking lots. The rate of crime attempts is a reasonable metric for determining the effectiveness of the security solutions in discouraging and reducing the crime opportunities.

If the criminals decide to commit crime anyways, despite the discouraging SCS solutions, we enter the second phase in the crime process. Now the security goal is no longer to discourage crime but to protect the integrity of the supply chain by keeping criminals away from cargo, infrastructure, and vehicles. The central concept, the supply chain integrity, is here defined as the state of being free from criminal exploitation. The integrity is typically protected with physical barriers – burglar resistant doors, windows, and fences, tamper-resistant packaging, and reinforced truck and trailer structures – that are designed to slow down the intruders. In general, the longer a barrier is able to resist the intruders, the more effective it is[27]. Because persistent intruders tend to penetrate through any barrier, if given enough time and right tools, protecting the supply chain integrity calls for capabilities for detecting and intercepting any unwelcome visitors. These capabilities are supported by a range of SCS solutions, including CC-TV system, burglar alarms, guarding, hotlines for reporting suspicions, GPS-based cargo tracking devices, and security escorts. Another aspect in the integrity preservation is to protect supply chain assets from internal threats posed by dishonest employees, business partners, or authorities – the supply chain insiders. To mitigate the first risk of having untrustworthy people on one's payroll, organizations commonly vet backgrounds of new recruits (e.g., criminal record and history of drug abuse), arrange managerial supervision, and follow a secure procedure when terminating work contracts (e.g., prompt return of keys and ID badges). The third risk of dishonest business partners is often mitigated through security auditing at partners' premises, cargo / document inspections at the moment of handover, and common-sense avoidance of dubious business deals. A relevant measure for determining the level protection is rate of security breaches – the frequency incidents breaking the supply chain integrity.

When the protective solutions fail, and the supply chain integrity breaks, it is still possible to foil crime attempts and restore the integrity before the situation escalates – bombs explode,

[27] A team of professional burglars with crowbars, for example, breaks faster into a warehouse than let say opportunistic drug addicts with improvised tools.

smugglers get their contraband through, or burglars escape with loot. Again, the physical barriers and the alarm mechanisms help react to anomalies and hinder and catch escaping intruders. In case of smuggling, when illegal goods are already travelling through the supply chain, and when the smugglers are no longer anywhere near their contraband, an effective way to foil the smuggling attempts is to risk assess, screen, and inspect the cargo traffic. The risk assessment determines urgency and need of follow-up controls by contrasting cargo information against predetermined high-risk indicators that signify possible elevated risk of smuggling. Common screening techniques include a variety of non-intrusive imaging techniques (often based on X-rays, gamma rays, neutrons), searches with sniffing dogs, material trace detection tests, and radioactivity measurements. Screening rarely yields conclusive evidence of the presence of suspected contraband, but it rather determines need for further screening with higher intensity or complementary method(s) or physical examination of shipping documents, vehicles of transport, or cargo (e.g., unpacking container for visual inspection). Often only results of the physical cargo examination warrant seizures. The detection probability is a reasonable measure for determining the effectiveness of the SCS solutions after the supply chain integrity has already been broken.

Investigative SCS solutions start playing the leading role in the SCS management the moment crime escalates (i.e., adverse consequences realize). The general goal of the investigations is to recover from the crime, and this goal can be split into four sub-goals. First, if the investigations succeed to identify offenders, the victims of crime (or their insurers) might get compensated for their losses. Second, successful criminal investigations signal potential offenders that crime does not pay off as most offenders get pursued, arrested, and punished. The third purpose is to uncover and fix weaknesses of contemporary security systems and this way prevent similar security breaches from recurring. The fourth and perhaps the most important goal of the investigative effort is to reduce the scope and the duration of supply chain disruptions that often follow major crime incidents, especially terrorist attacks. Many investigative SCS solutions overlap largely with the techniques that help detect and intercept crime attempts. For example, tamper-evident devices (e.g., seals and tapes), geolocation solutions (e.g., GPS tracking), or camera surveillance help detect signs of the broken cargo integrity, but also to investigate time and location of the crime incident, identifying details of the offenders, and the way they executed their crime. Investigation-only solutions exist as well, for instance internal theft detectives. Metrics for measuring the performance of the investigative efforts include the rate of offenders arrested, the speed of arrest, and the amount of losses compensated. Figure 3 illustrates the four-phase depiction of supply chain crime, the primary objectives of the SCS

solutions in each phase, and the decisive moments that divide the overall process into the distinct phases[28].

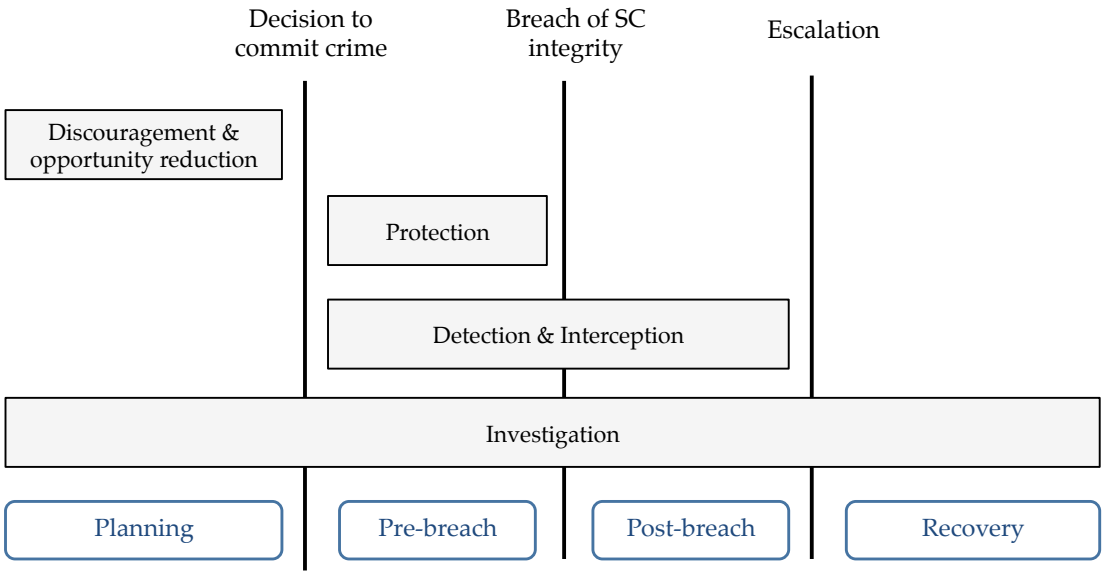


Figure 3 Phases of supply chain crime, decisive moments, and goals of SCS solutions

The literature synthesis suggests that the main goals of the SCS solutions and the dimensions of the SCS performance are discouragement & opportunity reduction, protection of cargo integrity, detection & interception, and investigation. Overall, the SCS performance, depending on the performance dimension, can be measured in terms of the rate of crime attempts (discouragement & opportunity reduction), the rate of foiled crime attempts before the supply chain integrity gets broken (protection), and the rate of foiled crime attempts before the crime escalates (detection & interception). The metrics for measuring the effectiveness of the investigations include the percentage of offenders arrested, the speed of arrest, and the percentage of losses compensated.

3.3. Effects of supply chain security

This section starts with a general outlook on the effects of the SCS implementation in general. Next it discusses how the SCS solutions influence the speed and predictability of the transport logistics and the dimensions of the SCS performance.

[28] It should be noted that many SCS solutions play a role in more than one phase and thus contribute to the general goal SCS management – the mitigation of the crime risk – by different means.

3.3.1. General effects

The implementation of the SCS solutions seems to have numerous effects on businesses, authorities, and the society at a whole. Perhaps the most obvious effect is that most SCS solutions cost money. Cost is a key factor in all reviewed shipping container inspection literature: some papers estimate the cost of the security implementation per site (Bakir 2011; Wein et al. 2006) while others calculate more precise cost-efficiency metrics such as inspection cost per container (Bakshi and Gans 2010; Bakshi et al. 2011). But core in all the analyses is the cost-effectiveness, which indicates how much risk reduction can be attained per dollar spent. The cost-effectiveness has been of a great interest also outside the container inspection literature. Using expert judgments as input, Urciuoli (2009) calculates net-present values of a set of anti-theft solutions and concludes that sound barriers (= noisy alarms), mechanical locks, and reinforced trailer structures provide most security for a given investment. Gutiérrez (2007) maps security solutions into four quadrants, based on their effectiveness and cost. Instead of searching cost-efficient solutions, some scholars have focused their attention on finding ways to share monetary costs of SCS investments between governments and the private sector (Sheu et al. 2006; Bakshi and Gans 2010) and among supply chain partners (Lee et al. 2011).

The SCS solutions affect business performance and many aspects of every-day logistics. Concluding from interview data, Autry and Bobbit (2008) argue that the SCS solutions "could result in supply chain risk management-related efficiencies, such as decreased lead times to customers, greater product reliability, waste reduction, and increased delivery reliability, due to the lessened need for operations workers to perform security-related tasks such as redundant container checking, securing shipments, or other similar tasks." Sheu et al. (2006) consider that the SCS implementation can improve or decrease customer satisfaction, depending on whether the chosen security solutions help or hinder a company to deliver goods in time, in right quantity, and in faultless condition. Both practitioners and academics have debated over collateral benefits of the SCS implementation on logistics and business operations. Rice and Spayd (2005) argue that security-motivated investments in track & trace solutions enable better planning and unlock potential for efficiency gains. They also suggest that security could lead to better customer satisfaction and higher brand protection (see Table 10 for further details). Sternberg et al. (2012) observed that adoption of a set of IT-enabled SCS solutions eliminated logistics efficiency and security issues simultaneously:

- Real-time geo-positioning of trucks and trailers enabled the port operator to allocate a vacant spot for a trailer prior to its arrival, which reduced the waiting time at the port entrance. The real-time information enabled also customs to detect anomalies in shipping schedules and routings that would imply a heightened risk of smuggling.

- RFID-based identification of drivers, trucks, and trailers automated and accelerated the access formalities at the port entrance and increased reliability of driver authentication.
- Digitalization of cargo manifests eliminated the time-consuming manual document handling and reduced the risk of unauthorised access to confidential information.
- E-seals enabled customs officers to identify intact containers and spare them from time-consuming inspections.

The SCS implementation mitigates the risk of crime-triggered supply chain disruptions and thus increases the managers' confidence in business logistics. If the confidence is warranted, the managers can capitalize on it by cutting spare production capacity, slashing safety stocks, shortening safety lead time, and lowering other safeguards that shield business operations from the supply chain disruptions (Lee and Whang 2005). Following the same logic, conversely, managers dealing with insecure, disruption-prone supply chains often must build redundancy to cope with problems stemming from unreliable logistics.

Investment	Collateral Benefits
Asset visibility & tracking	Fewer delayed shipments
	Faster product recalls
	Better planning, enabling lower working capital for inventory
	Less overages, shortages, and damages
	Protection of brand name
Personnel security	Customer loyalty, resulting in increased sales revenues, and higher market share
	Employee commitment and belief in company's concern for its employees

Table 10 Examples of collateral benefits of SCS investments (reproduced from Rice and Spayd 2005)

A common concern is that the security implementation, especially in the form of mandatory regulations, distorts fair competition. At the global scale, the local SCS requirements may redirect and reduce international trade flows. Security-concerned nations may be less preferable partners to trade with due to high security compliance burden they induce on importers and exporters. The "security spaghetti," a term coined by Grainger (2011), aptly illustrates the possible disarray of security policies, controls, and requirements that makes it less interesting for companies to engage in international sales and sourcing. More locally, Hintsa et al. (2010b) raise concerns that the security requirements burden more small and medium size enterprises (SMEs) than bigger companies, which tend to have more in-house security expertise and benefit from scale benefits also in security compliance matters. Due to the relatively higher compliance

costs, the SMEs end up in a competitive disadvantage vis-à-vis their bigger competitors. If the SMEs decided not to invest in the SCS implementation, they would find themselves in a predicament where they lose business deals due to inferior security levels (Autry and Bobbit 2008).

The literature strongly suggests that the SCS solutions have broad implications beyond the crime risk mitigation, monetary costs, and business performance. Haelterman (2011) provides perhaps the most comprehensive account of costs of the SCS implementation. He argues that practitioners should consider a set of non-monetary costs when they assess benefits and shortcomings of the SCS solutions. He agrees that security investments often involve a fixed one-time cost and continuous variable cost, but he also adds ethical, social, and esthetical costs to the discussion. The ethical and social costs arise when the SCS solutions label, discriminate, or denounce individuals or social groups. The discrimination occurs for example, when an organization refuses to hire anybody belonging to a certain social group because of past deviate behavior of one group member. Haelterman (2011) also mentions (increased) distrust between the management and the labor as a variety of the social cost, which arises from the intrusive SCS solutions such as background vetting, and searches on employees who leave facilities (an anti-pilferage measure). In a broader picture, Haelterman (2011) highlights that the SCS management sometimes undermines the civil rights. Especially the right to privacy gets sometimes sacrificed in the name of security, for example in case of the full body scanners at airports. Another example of a social cost is possible health implications of X-ray and other screening methods using ionizating rays or particles that may expose screening staff to elevated risk of contracting radiation-related illnesses (Sowerby and Tickner 2007). As regards to the esthetical cost, window bars, security glasses separating clerks from clients, and armed guards make environment less comfortable and welcoming.

Haelterman (2011) also discusses reverse effects of the SCS solutions. Among other SCS scholars (e.g., Ekwall 2009b; Murray-Tuite and Fei 2010), he highlights the possibility of crime displacement, in which offenders do not stop committing crime but change their criminal behavior in response to security solutions. The theory on crime displacement assumes that the criminals are rational agents who weigh risks and costs of crime opportunities against expected crime rewards, and that the displacement is likely to occur when supply of crime is inelastic[29], opportunities for crime are manifold, and potential offenders are able to observe changes in security systems and adapt their activity accordingly. The theory recognizes six types of crime displacement (Barr and Pease 1990; Hakim and Rengert 1981):

[29] If supply of crime is inelastic, criminals are insensitive to changes in local security defenses. For example, when crime opportunities are blocked, professional "career" criminals are more likely to search for new crime opportunities than their opportunistic less professional colleagues.

- Temporal – change of time when offenders carry out a crime (e.g., daytime → nighttime)
- Spatial – switch from targets in one location to another (e.g., warehouse → parking lot)
- Target – change of type of target (e.g., TV sets → microprocessors)
- Tactical – use of alternative method (e.g., pickpocketing → robbery)
- Offense – switch from crime to another (e.g., drug dealing → money laundering)
- Offender – a new offender takes a place of arrested or deterred earlier offender

In the supply chain context, studying changes in cargo theft rates, Ekwall (2009b) argues that professional cargo thieves seem to target increasingly "cargo on-wheels" instead of warehoused goods. He explains this shift in the behavior with the fact that, facility security has improved relatively more than in-transit security over the past decade. However, he stresses that it is hard to establish a causal relationships between security interventions and changes in criminal behavior. He holds further that if displacement occurs, it is likely to be partial rather than complete. In the analysis of Haelterman (2011), the tactical displacement, when it involves a shift from non-violent to violent methods, is called escalating effects. An example of the escalation, when crime prevention efforts make things go from bad to worse, is when car thieves go after the driver if they cannot steal a car without keys. Or when a client, who visits a post office to pick his mail from a formerly anonymous poste restante address, threatens a post office clerk who unexpectedly asks the client to prove his identify. Two major reverse effects are creative adaptation, when security activities disclose the criminals information about vulnerable targets, and the enticement effect, which occurs when copycat criminals commit crime the way they are described in the media. Sometimes new SCS implementation exposes organizations to new kinds of security threats. For example, converting paper documents into digital data certainly increases productivity of the everyday logistics as it reduces manual labor. However, the digitalization can expose the supply chain to new sources of disruptions, including cyber attacks, technical failures, blackouts, and sabotage.

The opposite of the geographical crime displacement is the diffusion of crime prevention benefits, also known as halo, bonus, and free-rider effect. The diffusion of benefits occurs when crime reduces in areas outside of the designated target of crime prevention efforts. For instance, research suggests that tracking devices, that allow car owners locate their vehicles remotely in real time, reduces crime of *all* cars, not just the ones that have the tracking device installed (Ayres and Levitt 1998). One explanation of this diffusion of crime prevention is that because potential thieves cannot know which cars carry the tracking device, the risk of getting caught and punished for stealing *any* car is higher. The higher risk discourages car thefts, at least among rationally thinking car thieves.

Altogether, though the cost-effectiveness has been a key topic in the SCS academic literature over the past ten years, the scholars seem to acknowledge that the SCS implementation has

important effects beyond the rather the cost implications and the crime risk mitigation. The literature talks much about so-called collateral benefits of SCS investments that may realize in terms of higher customer satisfaction, fewer damages on cargo, better brand protection, and so forth. It is also suggested that the SCS implementation can distort fair competition within industries and hinders international trade. Introduction of new security solutions may also change criminal behavior, possibly resulting in displacement of crime or in diffusion of crime prevention benefits.

3.3.2. Effects on logistics performance

Some SCS solutions slow down logistics. Bakshi et al. (2011) show that cargo inspections extend the transportation leadtime because shipments lose time as they (i) are moved to an inspection site, (ii) queue for inspection to start, (iii) pass inspections themselves. Depending on the location of the inspection site, the movement of cargo can waste a significant amount of time. Also queuing can extend leadtime remarkably, especially in congested systems. According to Gaukler et al. (2012), container inspection with a radiography technique takes 90 seconds on average, the inspection time being exponentially distributed. An average inspection with passive radiation detectors, they continue, takes around 45 seconds. If a container fails the radiography screening and the passive radiation test, it is directed to a one-hour-long physical inspection, in which inspectors open and unpack the container to examine its contents manually. Bakshi et al. (2011) suggest that a combined X-ray inspection and radiological detection takes on average 20 minutes per container under the inspection regime of the Container Security Initiative (CSI).

Security-related uncertainty is detrimental to logistics. Under so-called risk-based inspection regimes[30], authorities select only a certain percentage of traffic to inspection, so logistics operators can rarely be certain whether or not their cargo gets inspected and thus delayed. In fact, the less common and the more random the inspections are, the bigger the surprise is when the inspections eventually occur. For example, because customs inspections are almost non-existent in the intra-EU traffic, shippers commonly view the inspections as exceptional, unanticipated contingencies that may delay the shipment from its planned schedule. By contrast, under the 100-% screening regimes, under which every single shipment faces inspection, security-related delays are inevitable, expected, and often predictable. Besides the chance of facing inspections, the variable inspection time is another source of uncertainty. The shipper does not know how much time the security procedures are going to take. The duration

[30] Except for few one-hundred-percent screening regimes, which are deterministic and thus predictable, all screening system involve a degree of uncertainty. With some exemptions, the global air cargo security is an example of the 100-% inspection policy.

of the inspection varies according applied inspection techniques, skills of inspection staff, and most importantly the current congestion of the inspection system, which determines how long a shipment must wait for inspection. In addition to the queuing time and time it takes to pass the inspection itself, the trip to the inspection facility adds variability to the inspection time. Table 11 illustrates some average inspections times of certain commonly used shipping container inspection techniques.

Source	Technology	Average inspection time (distribution)
Gaukler et al. (2012)	Radiography machines	90 seconds (exponential)
	Passive radiation detector	45 seconds (constant)
	Manual inspection	1 hour (exponential)
Bakshi et al. (2011)	"Scans with radiation isotope identification devices (RIIDs) are used to detect radioactive emissions; and radiographic imaging, using high-energy (9 MeV) x-ray equipment"	20 minutes (lognormal)
	Drive-through NII scan using medium-energy x-ray radiography,	25 seconds (constant)
	ASP scan	45 seconds (lognormal)

Table 11 Durations of shipping container inspections with different techniques

Logistics gets also delayed due to physical security measures, which protect supply chain assets and facilities from unauthorized people. Authorized supply chain actors lose time in clearing entry protocols before entering logistics facilities. Sternberg et al. (2012) found that it takes 10 minutes and 11 seconds on average for a truck to enter a seaport, if the driver needs to pass a conventional entry protocol involving documents checks and a face-to-face conversation with the gatekeeper. The time lost includes durations for four sequential entry activities: preparation of entry documents (01:14), check-in (07:01), waiting access to be granted (00:54), and opening the gate (01:02). Considering that an average international shipment travels through numerous logistics facilities (e.g., ports, warehouses, customs offices etc.) and is subject to dozens of handovers during this journey, the entry protocols collectively have clearly a consequential negative impact on the average transportation time and on the transportation time variability.

The literature suggests that sharing of security-related information may be detrimental to the on-time delivery performance (Bakshi et al. 2011). Certain government regulations rule that traders share cargo information with customs way before the customs get the custody over the

goods (e.g., data is sent when the cargo is still in transit or waiting to be loaded on a vehicle of transport). If the traders or their representatives fail to lodge this information by formal submission deadlines, the delivery of the cargo gets blocked and the delivery falls behind the planned schedule. The delay can be significant: the US National Association of Manufacturers (NAM) estimates that the US "24 hour manifest rule" adds three full extra days to the time an average container spends in a port before being shipped out for the US (Field 2009). Stringent data submission deadlines may also extend the shortest possible delivery time. Because of the US 24-hour rule, Bakshi et al. (2011) explain, any container must wait at least 24 hours in a port before it can be shipped out. Thus not even the most urgent "hot boxes" can be loaded onto ships immediately, as soon as they enter the port.

Security concerns sometimes affect routing and scheduling decisions, especially when crime-prone cargo is shipped. If route alternatives exist, logistics managers might avoid shipping alongside the Somalian coast, a region notorious for rampant sea piracy. Alas, avoiding the shipping through the pirate-plagued hotspots requires detours, and the detours often induce extra shipping cost and extend the shipping time. And if the high-risk shipping route cannot altogether avoided, the managers need to plan extra security measures, such as stops at off-route secure harbors (or parking lots in case of road transport) with possible delays. There is also a risk that terrorists could capture a load of hazardous cargo (e.g., sulfur acid) and use the load to mount an attack. Considering this possibility, Reilly et al. (2012) suggest that governments could start regulating routing and timing of hazardous cargo shipments for *security* reasons in addition to the currently effective safety regulations.

Maybe the most powerful security-related supply chain disruptors are new regulations and restrictions that governments introduce as emergency measures in response to major security incidents, most notably terrorist attacks (Sheffi 2001). In the immediate aftermaths of the 9/11 terrorist attacks, government authorities closed the US borders and the airspace for three days. The resultant disruptions in the US-bound cross-border cargo flows soon affected manufacturing and retailing. Automakers Ford, Toyota, and Chrysler, for example, were forced to stop their assembly lines intermittently as their component replenishments got delayed at the Mexican and Canadian borders (Sheffi 2005). Meanwhile at the airports worldwide, air cargo and mail deliveries were blocked. When the airspace was opened again, it took more than two weeks to clear the backlog (David and Stewart 2010). Another abrupt security response took place in October 2010 when al-Queada terrorists shipped two explosive devices out from Yemen onboard passenger planes. Although the authorities managed to intercept and defuse the bombs in time, governments, especially in the western countries, introduced traffic restrictions and new unprecedentedly stringent air cargo security requirements. The new security regime changed the air cargo and mail operations overnight, seriously disrupting the global air cargo and mail traffic. The delays were widespread and lengthy, but the worst aspect

of the disruption was that no one knew when the new apparently transient security regime was to be revoked.

No doubt, the SCS implementation sometimes helps reach higher on-time delivery performance. We concluded in the previous section that high overall security discourages some potential criminals from attempting crime, and strong and visible protective security solutions stop a percentage of crime attempts before the supply chain integrity gets broken. Logically, a lower crime rate implies a lower likelihood of security breaches and thus a lower likelihood of crime-triggered supply chain disruptions. This means, in other words, that the SCS implementation improves chances that shipments get to the intended destination without being stolen, tampered, or delayed along the route. And even if a security breach occurs, the SCS solutions, cargo inspection techniques in particular, can still detect and intercept to avoid disruptions, or at least mitigate their impact[31]. Investigative SCS solutions do not reduce the likelihood of disruptions as much as they delimit the magnitude of the crime-triggered supply chain disruptions (Lee et al. 2011). Capability for effective investigations speeds up location of sources of security threats, identification of suspects, and description of the method used to execute the crime (i.e., modus operandi). This investigative evidence allows authorities to confine their responsive measures only to necessary trade routes, traffic types, and logistics actors and to design emergency measures, which are proportional to the threat. For example, after the mail-bombing spree against embassies in Athens in 2012, based on the initial investigation results, Greek authorities decided to suspend the international letter and parcel services for 48 hours instead of closing the entire postal and express courier services. In the Greek case, fast investigations resulted in rapid arrests that helped restore the public confidence in the letter and parcel delivery service and justify relatively fast revocation of the emergency measures.

Sometimes, voluntary SCS compliance makes companies eligible for privileges that help them expedite logistics and thus improve the on-time delivery performance. By investing in SCS, a firm signals its intention to act like a good corporate citizen, and this signal helps foster its relationships with customers, authorities, investors, and other stakeholders (Williams et al. 2009a). Indeed, the SCS investments, and the goodwill it brings, may bring more business opportunities (Hintsa et al. 2010b) and result in lower government scrutiny, like less frequent inspections at borders (Prokop 2012). More precisely, voluntary compliance with security-centric Authorized Economic Operator (AEO) programs allow, at least on paper, the compliant companies to enjoy a variety of "club benefits," including streamlined customs (security)

[31] It is true that often when bombs, biological weapons, or deliberately contaminated products are detected and intercepted in the supply chain, disruptions occur in any case due to emergency measures authorities take to prevent such threats re-entering the supply chain.

formalities, lower risk of facing security inspections at the border, and even priority "green line" treatment through border crossing (Hintsa et al. 2010b). The voluntary SCS compliance can be seen as a partial insurance against major crime-triggered supply chain disruptions: it is likely that authorities would grant security-certified companies a "restart priority" and allow them to be the first ones to resume logistics operations in the aftermaths of a terrorist attacks or other disaster (Bakshi and Gans 2010; Prokop 2012). In a study of Sheu et al. (2006) on real effects of the club benefits, four out of five C-TPAT compliant companies reported having experienced faster inspections at borders, reduced costs, and higher customer satisfaction since they joined the C-TPAT program. JC Penney, one of the five case companies, claimed that, after the C-TPAT implementation, the inspection rate of their cargo fell below the industry average of six percent. A survey of 814 US importers reveals that 35,4% of the respondents observed lower rate of border inspections over the year following the C-TPAT implementation[32] (Diop et al. 2007).

This section reviewed why the SCS implementation is often said to disrupt the day-to-day logistics, making it less reliable. We found that the cargo inspections, entry protocols, security-motivated information requirements, and the security-affected routing decisions indeed extent transport time and transportation time variability. On the other hand, the literature synthesis suggests that the SCS implementation protects the supply chain from serious crime-triggered disruptions by lowering the likelihood of crime and reducing the scope and the duration of the disruptions. Also benefits of voluntary compliance with SCS initiatives, including the restart priority or the fast green line customs treatment, help companies reach higher logistics performance.

3.4. Principles of logistics-friendly security

This section discusses themes and principles of logistics-friendly design of SCS systems. Like the previous section, the following analysis stems from the previous synthesis of the peer-reviewed academic literature.

3.4.1. Mix of solutions

The academic literature strongly suggets that there are some important considerations to which decision makers should pay attention when selecting security solutions. It is important to consider that the combined effect of two or more security solutions is sometimes greater than the sum of separate effects of each solution. A standalone CC-TV system, for instance, may deter crime and facilitate investigations, but when the system is coupled with guards, who

[32] 6.6% of the firms observed higher inspection rates and 44,1% observed no change.

constantly monitor the cameras, the CC-TV system also helps intercept unwelcome intruders. Synergies emerge as the guards improve the performance of the camera system, and vice versa. In the container security screening, the combined use of radiation detectors and X-ray equipment (or other imagining technique) detect radiological and nuclear threats with high accuracy whereas the use of either technique separately yields rather inaccurate results. The functioning of the combined system is rather simple: the radiation detectors identify those high-risk containers that emit exceptional amounts of radiation. The complementary X-ray screening, in turn, identifies containers that do not necessarily radiate much because they are packed with lead, steel or other dense materials that may shield a concealed source of radiation and thus prevent radioactivity from escaping from the inside of the container. When comparing the intensity of the observed radiation with the amount of the shielding material, inspection officers can identify and select the most risky containers for further controls. Making the follow-up screening decision based on the radiation-shielding ratio decreases the frequency of false alarms without lowering the crucial detection probability (Gaukler et al. 2012).

Layered security is another example of the complementariness of the SCS solutions. A common wisdom among security expert is that 100% secure supply chain is an elusive ideal that can never be achieved. The reasoning goes that eventually, criminals beat any single security solution because of their perseverance, luck, cunning, and skills. To diminish the criminals' chances, the experts often design security systems that comprise multiple independent protective layers. For example, the US maritime SCS has a layered design that is built on multiple SCS solutions: the source control (trusted trader programs such as the C-TPAT), physical measures to secure port and ship facilities (the ISPS code), tamper-evident security seals, risk scoring (with the 24-hour manifest data), container screening at the port of departure (the CSI initiative), and the complementary screening at the port of destination. None of the protective layers eliminate the risk that terrorists would smuggle a nuclear bomb or other devastating weapon into the US in a sea container. But together these layers constitute a strong protective system that, at least to date, has succeed to prevent extreme maritime terrorism[33]. In other words, a layered system is a robust system: one or more failing layers do not necessarily lead to a security breach.

It is important for security and logistics performance in which sequence security controls are arranged (Van Weele and Ramirez-Marquez 2011; Merrick and McClay 2010). As a rule of thumb, it is reasonable sequence controls so that large volumes of traffic get screened with fast techniques. Later, after the primary control, only those shipments that raise an alarm would be

[33] The High Reliability Theory provides another analogy: potentially hazardous systems, such as nuclear power plants, must be secured with multiple independent safeguards to avoid small problems, which inevitably arise in complex socio-technical systems, and which, in unfortunate combinations, escalate into a major disaster.

inspected with slower but more thorough screening techniques. The labor-intensive manual inspection would be the last resort. This kind of inspection system, that involves a quick primary inspection and conditional, more time-consuming follow-up inspections, enables the bulk of the traffic to pass controls fast; delays would concern only high risk traffic, that would likely account only for a fraction of the total traffic. Such converging controls systems are increasingly used in border controls. Customs typically risk assess all traffic (by comparing declared data against risk profiles) but block perhaps a percent of shipments / consignments so that they can examine them later, for example with narcotics detection dogs. Based on results of the canine search, customs officers might decide to examine visually two percent of the shipments (and related documentation). Finally, only one percent of the shipments would be opened and manually examined. Importantly, the customs officers and other controllers could decide the need for the follow-up controls dynamically case-by-case, based on the prevalent security targets and congestion of the control system.

Many times more than one threat is targeted in a single cargo inspection exercise. In such cases, besides the fast-to-slow screening sequencing, it is reasonable to move from multi-threat inspection techniques towards more specialized techniques. The first screening would be able to detect a broad range of threats, let say all commodities that differ from the declared cargo contents. The subsequent screening techniques would be specialized to detect a specific kind of contraband. For example, X-ray screening produces an inside view of an object and thus allows screening operators to recognize atypical shapes and materials that do not correspond the declared contents. If this primary X-ray screening raised suspicions about narcotics, the screening operators might bring drug-sniffing dogs to corroborate the initial findings. If the dogs also raised an alarm, as the last measure, the operators might decide to proceed to manual inspection, in which they would manually open shipments, disassemble truck structures, or do whatever it is required to get a physical access to the suspected drugs.

The literature also proposed that so-called risk-based security implementation is the most-effective way to secure the supply chain. The idea is to assess risk levels of different supply chain entities – shipments, companies, logistics facilities, shipping routes, and so forth – and secure each entity with security measures that are proportional to their risk level. Central to the risk profiling exercise is to identify factors that indicate elevated security risks. In case of route profiling, for example, apparent high-risk indicators include length of the route, number of logistics middlemen, and attractiveness of cargo to theft (e.g., electronics or brand apparels) or hostile tampering (e.g., food products). After the high-risk indicators and their relative importance have been defined, it might be possible to calculate a risk score for each shipping route (or whatever supply chain entity is to be profiled). The more accurately properties of the entities match with the high-risk indicators, or cluster of them (known as risk-profiles), the higher the risk score grows. The risk scores allow further ranking and categorization of the

entities by security risk level (see a more detailed illustration of risk scoring in Box 4). The exercise reveals the most vulnerable entities to protect and helps effective and proportional allocation of budgeted SCS resources – staff, equipment, and expertise – across investment options. To secure a high-risk shipping route, for instance, a logistics manager might introduce security escorts, schedule stops only at secure parking lots, employ GPS tracking devices, or other special in-transit security measures. In vulnerable facilities, it is common to introduce advanced physical security solutions such as 24/7 guard patrols and biometric access control systems on top of fencing, locking, camera surveillance, and other baseline security measures. To sum up this sub-section, Table 12 compiles design principles of logistics-friendly SCS management that are related to the mix of solutions theme.

Design principle	Main literature evidence
Look for complementary security solutions that provide synergies	Joossens and Raw (2008), Lee et al. (2011), Bakshi and Gans 2010, Van Weele and Ramirez-Marquez 2011
Consider sequence of security solutions (sensors)	Van Weele and Ramirez-Marquez 2011, Merrick and McClay 2010
Adjust alarm thresholds dynamically to meet desired security level and to cope with system congestion	Belzer and Swan (2005), Autry and Bobbit 2008; Voss et al. 2009b, Martens et al. 2011
Pursue risk-based security implementation	Gaukler et al. (2012)

Table 12 Mix of solutions: design principles and evidence

In the air cargo and mail security domain, the objective of risk scoring (also known as risk assessment or "soft screening") is to identify those shipments that pose the highest risk to aviation security. The modern risk scoring is based on advance electronic information (AEI) that contains information on routing, declared contents, shipper, and consignee, among other cargo-related data elements. In the risk scoring, these data elements are crosschecked against each other for internal consistency and against external databases for external consistency. The consistency indicates whether the data is to be trusted. Does the weigh of the shipment correspond declared commodity and quantity? Does the shipper exist in commercial registers? Is the phone number of the shipper real and has it been used recently? The next step is to analyze internal risk factors. Is the declared commodity commonly used to conceal contraband or security threats? Does the declared commodity make sense with routing? Finally, the data elements are contrasted against external databases to find out whether they raise security concerns. Does the shipper have a track record of compliance? Is the recipient on the list of terrorist suspects? Altogether, the final risk score is the function of the internal and external consistency as well as the internal and external risk checks. If a cargo movement corresponds a risk profile, a cluster of connected high-risk

indicators, it is typically selected for screening and/or examination[34]. Figure 4 below provides a stylized illustration on how one can calculate the risk score for an airmail shipment that is controlled for explosives[35].

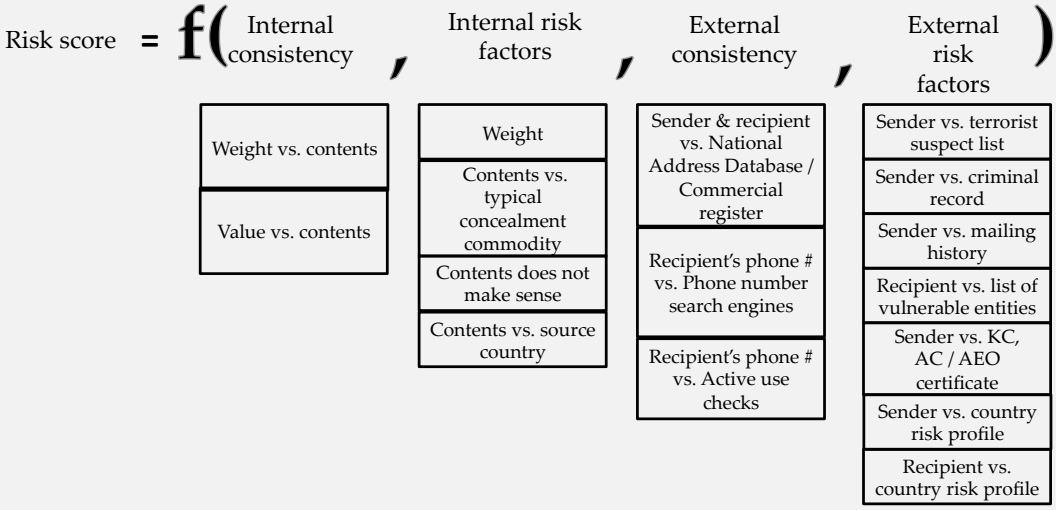


Figure 4 Stylized airmail security risk scoring logic[36]

Box 4 Risk scoring logic in the air cargo and mail domain

3.4.2. Logistics integration

The SCS scholars and practitioners agree that security solutions should be integrated into the supply chain with least possible disruptions to routine operations. However, there is a fierce debate about how to reach this condition of "least possible disruption." Many of the scholars suggest that the extent of disruption stems mainly from the location of cargo inspections in the supply chain. The common argument is that the sooner cargo gets controlled in the supply chain, the better it is for the security and logistics performance (Russel and Saldanha 2003; Lee and Whang 2005). Arguments against pushing screening towards the upstream supply chain[37]

[34] A wide range of follow-up controls exist, the most important being basic screening, intense screening (multi-methods and/or higher intensity) or Do Not Load instructions.

[35] There are four general logics for selecting shipments for inspection: random, rule-based, score-based, or a combination of them. For example, customs officers may have instructions to screen all US-bound shipping containers for radioactive material (= rule-based logic) and other containers if their risk level exceeds a predefined threshold (= score-based logic). From time to time, some low-risk containers may face random inspections despite the fact that rule- and score-based selection strategies are applied.

[36] Illustration inspired by "TSA Cargo Security Program" presentation held by Pam Hamilton in March 2005.

[37] The term "source control" is common in the academic SCS parlance. In my view, however, the source control term is somewhat misleading because the idea is not always to move controls all the way up to the source, to the origin of the supply chain, but rather to transfer control locations one or more steps *towards* the source. Therefore, in this thesis, for conceptual clarity, I use the term *upstream control* instead of the source control. It should be noted that the concept of upstream is relative as it depends on the position of an observer in the supply chain. From a consignee's standpoint, the entire supply chain before the final delivery is the

exist as well, highlighting cost and logistics implications that relocation of security controls may bring (e.g., Signoret 2011; Bakshi and Gans 2010). To summarize the arguments on the both side of the debate, it seems that many reasons affect the optimal location of the cargo controls in the supply chain. First, the urgency of targeted threat(s) dictates to a large extent where in the supply chain cargo should be controlled. Bombs and CBRN (chemical, biological, radiological, and nuclear) weapons can kill people and may cause damage *as* they travel through the supply chain. Besides, the more time these security threats spend in the logistics system, the more likely they are going damage somebody or something. Therefore, these threats should be controlled as early as possible in the supply chain. By contrast, illegal drugs, unlicensed firearms, counterfeit medicines, and most other contraband types call for less urgent controls than the security threats. Granted that illegal drugs may be dangerous when consumed, but at the time they are moved through the supply chain, they pose no risk to transport safety or security. They are harmless during transport, so there is no need to rush controls, and cargo can be controlled for whenever it is most convenient and most cost-efficient to do so. Figure 5 below summarizes this reasoning about the urgency of controlling various security threats and contraband types.

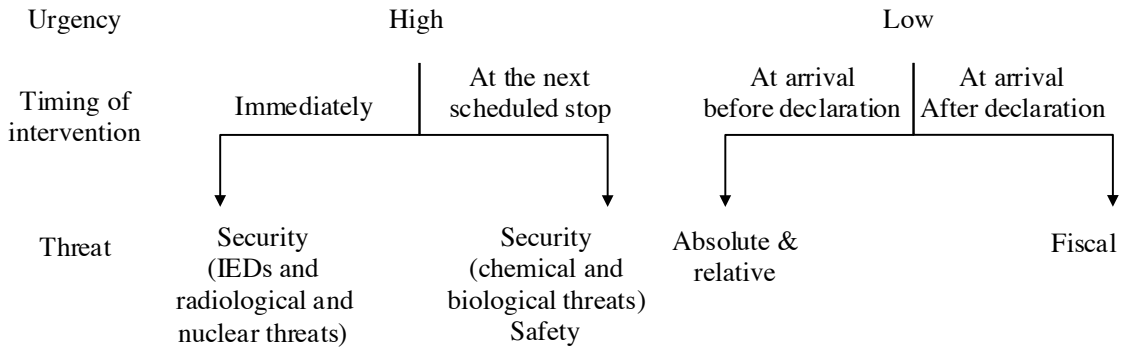


Figure 5 Urgency of control for various types of contraband and security threats

Second reason for pushing cargo inspections towards the upstream supply chain is to intercept threats before they enter a vulnerable section in the supply chain. The perception of vulnerability depends on the observer. The US authorities, for example, prefer to screen shipping containers already in oversea ports where possible security threats not yet endanger the US homeland security[38]. If a nuclear device or a dirty bomb was detected, the problem would be in a foreign country, and there would be no need to close US ports or deal with the

upstream. In contrast, manufacturers see raw material and component suppliers as upstream operators and wholesalers and retailers as downstream operators.

[38] Recall that the US government has introduced programs like CSI and SFI (Security Freight Initiative) and laws like the pending 100-% scanning that aim to "push the borders outwards" through relocation of container screening into foreign seaports.

precarious situation at the US soil. On the other hand, the relocation of inspections into overseas ports may reduce the risk in the country of destination but increase it elsewhere, in the country of origin or in transit countries. Moreover, the screening in the foreign ports costs significantly more money than screening in the US ports (Wein et al. 2006). In general, beyond the US centric view, it is not smart to bring high-risk cargo near cities or ship the risky shipments through vulnerable logistics gateways and hubs. If we were to discover a dirty bomb in a container at the outskirt of a large city, for example, massive evacuations would follow. A similar discovery in a major seaport would disrupt maritime logistics worldwide. Ideally, to avoid large emergency maneuvers, security inspections should be carried out in a remote, isolated location, let say, on an offshore inspection facility[39].

It should be noted that even if there was political will to control security threats in upstream supply chain, there would be certain resource and legitimacy constraints that might foil any relocation plans. As Haelterman (2009) points out, some countries might not have necessary infrastructure and know-how to support use of modern security technologies. Moreover, being short of real estate, many seaports and airports simply do not have room to accommodate inspection facilities. The second major constraint is legitimacy that enters the equation when authorities seek to enforce SCS outside their own jurisdiction. The lack of legitimacy is a major hindrance in SCS management especially on international waters, where coastal and flag states are having hard time justifying law enforcement controls in the absence of modern legal framework (Roach 2004).

The relocation of the cargo inspections has sometimes implications to security in the downstream supply chain. Secured air cargo, for example, must be protected from unauthorized tampering until it is safely loaded and locked into an aircraft's cargo hold. Protecting transport, handling, and warehousing activities that follow the inspection require reasonable physical security measures, clear protocol for distinguishing the secure cargo from the unsecure, and measures to assess trustworthiness of people who may have access to the secure cargo. On the other hand, early inspections might eliminate the need for screening later in the supply chain, where the screening activities might be unpractical. Particularly, if piece-level screening is required for higher detection accuracy, it is particularly useful to screen cargo before it is consolidated into aggregate units (e.g., pallets) or loaded onto vehicles of transport. In such cases, screening, that takes place before the consolidation, saves time and effort. Location of security controls into central facilities may also reduce the average cost of screened item because the overall cost of screening would be spread over a large number of items.

[39] Clearly, logistics challenges of directing traffic through an offshore screening site would be close to insurmountable.

Besides the location of screening in the end-to-end supply chain, it matters how security controls are integrated into the sequence of baseline logistics activities. Bakshi et al. (2011) illustrate the impact of the security integration on speed, cost, and predictability of the seaport logistics. They observe that security inspection at port entrances (quayside for ships and city-side for trucks) with drive-through inspection portals, does not delay nor divert the routine container handling process, in which a crane unloads a container from a ship or a truck and deposits it to a stack where the container waits until it is its time to leave the port. But if a container is inspected a few hours prior its scheduled departure, as is currently done under the US Container Security Initiative (CSI) regime, the routine handling process gets disrupted, (see Figure 6). Remarkably, the only value-adding security activity "non-intrusive inspection" (11) requires three preceding activities (8-10) and another three following activities (12-14), none of which add value from security or service standpoints. Other valueless activities, which do not appear in the illustration, include searching of the shipment selected for screening and verification of its documentation. The extra activities consume time and money but add no value to the shipping service. The first approach with drive-through portals eliminates the non-value adding supportive logistics activities (8-10 and 12-14) and therefore enhances logistics speed and efficiency without necessarily lowering the security level.

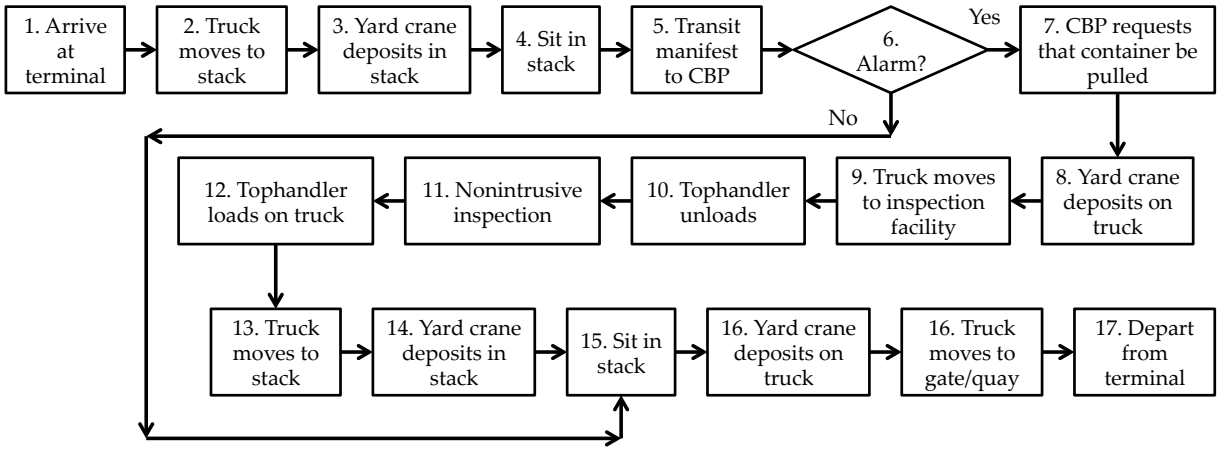


Figure 6 Container handling process under the CSI regime (Source: Bakshi et al. 2011)

Another way to streamline logistics is to get rid of duplicate controls. For example, it makes little sense to re-screen air cargo at transfer locations if the cargo has already been subject to equally rigorous screening at the origin or at one of the earlier transfer sites. Despite the re-screening is nothing but wasteful misuse of time, money, and resources, the duplicate security controls are a commonplace in the contemporary air cargo and airmail business because different countries do not recognize each other's security regimes. Parallel processing of security activities would further streamline the logistics process, making it faster and more efficient. It would be ideal, for instance, if officers from different law enforcement and other

regulatory agencies examined cargo at the same time so that the examined cargo could continue its journey as soon as possible. For example, health regulatory agency would control cargo for counterfeit medicines simultaneously with customs officers who would search for illegal narcotics. Naturally, any solutions that accelerate security activities or associated supportive logistics activities would contribute to logistics performance. Table 13 below summarizes design principles and related literature evidence that are related to the logistics integration theme.

Design principle	Main literature evidence
Consider substituting cargo screening for other security solutions (e.g., track & trace)	Sheu et al. 2006, Prokop 2012, Bakshi and Gans 2010
Eliminate redundant security solutions and associated supportive logistics activities	Signoret 2011, Bakshi and Gans 2010
Process security and logistics activities in parallel whenever possible	Bakshi et al. 2011
Accelerate process time of and queuing time to security processes	Gaukler et al. 2012 Bakshi et al. 2011

Table 13 Logistics integration: design principles and evidence

3.4.3. Capacity & intensity

The academic literature considers capacity and intensity of security systems as important parameters that affect security and logistics performance. Especially the shipping container inspection literature shows that when the volume of inspected cargo overwhelms the capacity of an inspection system (e.g., containers / hour), maritime logistics get congested and delays occur. Seaports would naturally like to have sufficient screening capacity, but the problem is that the screening capacity costs money in terms of equipment, installation, training, operation, and occupied real estate. There are basically four main factors that increase the need for screening capacity: the volume of traffic, security targets, productivity of screening resources, and logistics performance objectives. The traffic volume tends to fluctuate due to weekly and seasonal changes, economic trends, among other factors. The security targets determine the percentage of the traffic screened (e.g., only containers from certain high risk origins) and the intensity of the screening. The best productivity indicator of the security resources is the average time needed to screen cargo up to the targeted security level. Screening equipment, skills of the screening staff, and the type of the screened cargo largely determine the screening productivity (shipments / hour / screening site). The logistics performance objectives restrict the time cargo can lose in the overall screening process (queuing + processing). Speedy logistics

imply short queues and no congestion, and this speed can be achieved only with sufficient screening capacity that can handle the baseline volume and temporal volume peaks without congesting the screening system.

There are some ways to lower the need for the costly screening capacity. The first one is just to tolerate more congestion-related delays and accept worse logistics performance as the consequence. Another option is to lower the security targets by decreasing the screening intensity or by reducing the percentage of containers selected to the screening. This option would obviously diminish chances of detecting security threats. Many times, nevertheless, any (major) congestion is intolerable, and the security standards cannot be lowered. In such cases, when queues start building up, the only solution is to expand the screening capacity. A higher capacity can be reached by enhancing productivity of the existing screening stations or by increasing the number of the stations[40]. The first productivity approach requires more skilled staff or more advanced equipment whereas the second approach calls for more staff and equipment. Both approaches incur extra costs.

Perhaps the best way to deal with the capacity dilemma is to develop mobile, scalable, and modular screening resources that can cope with traffic fluctuations and changes in security policies. The mobile resources like portable explosive trace detectors or itinerant inspection teams could be deployed whenever local need for extra capacity arises. Solutions for making the security systems scalable include design of easy-to-learn screening procedures and development of fast-to-install screening technologies. The modular screening systems could be mounted with additional sensors that could be rapidly accommodated to detect new threats, for example a range of biological and chemical weapons. **Table 14** below summarizes the design principles related to the capacity and intensity of the security systems.

Design principle	Main literature evidence
Design modular security systems that can be adjusted to address new threats	Lee et al. (2011), Bakshi and Gans 2010, Bakshi et al. 2011, Merrick and McLay 2010
Design rapidly scalable security systems	Wein et al. 2012
Invest in mobile security solutions to alleviate congestions and to build early response capability	Bier and Haphuriwat (2011)

Table 14 Capacity & intensity: design principles and evidence

[40] The capacity of a process, a string of sequential activities, is determined by the activity with the slowest throughput rate (units / time) or inversely the longest cycle time (time / unit). Therefore, a multi-stage inspection system should have sufficient capacity at every inspection stage, or otherwise the system becomes a bottleneck of the overall logistics process.

3.4.4. Secrecy of information

The academic literature suggests that supply chain stakeholders should strike a balance between transparency and secrecy of security-related information. In particular, the stakeholders should decide what pieces of the security-sensitive information to share, with whom, and under what conditions. A good information disclosure strategy is to communicate general principles of security controls, but without revealing precisely how the security procedures eventually unfold. For instance, customs administrations could decrease the uncertainty involved in the cross-border logistics if they specified general rules of their border controls: How much time can customs officers take to inspect a shipment? How are conflicts resolved between the customs and the industry? The customs and other authorities could also notify logistics operators about upcoming inspections as soon as possible (Lee and Whang 2005) because such early information would give the operators time for proactive logistics and capacity planning (e.g., staffing, scheduling, and space allotment). If the customs communicated in advance that their officers would examine a particular consignment on arrival (e.g., timing, duration, and site of the control), a logistics operator could arrange an expedited connection for the examined consignment to offset the inspection-induced delay.

While the transparency of the security-information may improve the logistics efficiency, the disclosure of this information has its pros and cons from the security perspective. In general, conspicuous display of strong security systems discourages criminals from attempting crime (Bier and Haphuriwath 2011). Moreover, detailed information about the security systems underpins effective oversight of security activities and helps spot and fix security vulnerabilities quickly. On the other hand, if a security system was based on predictable and transparent rules, criminals and terrorists, being rational, learning, and adaptive antagonists, would find and exploit the system's loopholes eventually. By contrast, covert security solutions prevent the potential criminals from learning and exploiting the loopholes, but because of the hidden nature of the solutions, the covert defenses provide no to little deterrence for the very reason that the potential offenders are not aware of them. Moreover, because the criminals cannot plan ex-ante how to circumvent the covert security solutions, the hidden controls might have a higher chance of catching criminals red-handed than the overt security solutions (Merrick and McLay 2010).

Another good information-related practice is to modify security systems periodically. Changing procedures would reduce the time the criminals have to learn and exploit the weaknesses of the security system. Also employees might remain alert for security threats if they needed to learn regularly new security procedures. Besides the changing security controls, the security systems should be randomized to a degree, so that criminals could never find foolproof methods for committing crime. Finally, to maintain some discouragement and deterrence effect even if the

security controls were mainly covert, the authorities could boast successful law enforcement results, announce periods of intensive enforcement, and spread stories on how offenders always get caught and convicted. Such communication strategy would make people aware of effective law enforcement (or at least create an illusion of effectiveness) and deliver the message that crime does not pay off.

Another idea arising from the literature is to lower anonymity of the logistics service so that it would be hard to ship anything without revealing one's real identity. The anonymity often harbors people who misuse the logistics services for criminal purposes. The anonymity reduces likelihood that the abusers of the logistics services get caught and face sanctions. Assuming that the criminals are rational actors, the lower possibility of facing sanctions reduces the risk of crime and thus makes the potential criminals more inclined to commit crime. As another downside, the anonymity of the logistics service makes crime investigations more difficult. Table 15 concludes this sub-section by restating the design principles and supporting literature evidence on the secrecy of information theme.

Design principle	Main literature evidence
Share general information about security principles (e.g., max durations of inspections)	Lee et al. (2011), Bakshi and Gans 2010, Bakshi et al. (2011), Merrick and McLay (2010)
Randomize and alternate security controls to a degree	Wein et al. (2006)
Reduce anonymity of logistics services	Bier and Haphuriwat (2011)

Table 15 Secrecy of information: design principles and evidence

3.4.5 Collaboration & culture

The SCS literature strongly suggests that all the earlier themes and principles of the logistics-friendly SCS management are underpinned and reinforced by collaboration and security culture. There is a broad consensus among the academics that inter- and intra-organizational ability to collaborate on the SCS matters is critical for both logistics and security performance (Sheffi 2001; Closs and McGarrel 2004; Sarathy 2006; Russel and Saldanha 2003; Manuj and Mentzer 2008; Autry and Bobbit 2008). The collaboration literature helps find ways to incentivize people and organizations, which would not otherwise have sufficient interest to contribute to the SCS management, to engage in the fight against supply chain crime.

Let us briefly elaborate why some organizations lack the interest in taking part in SCS. Supply chain security (SCS), in the sense of counter-terrorism, is a public good because it brings

positive externalities, beneficial side effects to the society as whole (Prokop 2012). In economics, a public good is a commodity that is both "non-rivalrous" and "non-excludable". The non-rivalry means that consumption of a commodity by somebody does not reduce possibility of others to consume the same commodity. In the SCS domain, the non-rivalry means that the secure level remains the same irrespective of the number terrorist attacks a security system prevents. The non-excludability means that nobody can be excluded from consuming the commodity. The counter-terrorism SCS is a non-excludable product because local counter-terrorism efforts benefit the whole global trading community. In other words, a firm that invests in SCS, and thus lowers the risk of terrorism, does not reap all benefits from the investment as other companies (and governments) benefit as well, without having to pay anything. Such positive externalities arise because local security breaches often disrupt trade and logistics far beyond the immediate context where the breach occurs (Sarathy 2006). A terrorist plot involving explosive airfreight shipments, for example, would paralyze international air cargo deliveries and cause serious distress on airlines and a variety of companies (and their clients) that rely on the fast and day-certain air logistics. The companies face a free rider dilemma: why should they spend money on SCS themselves if they can benefit from the spending of the others? Due to the free rider effect, managers sometimes make calculated decisions not to invest in the SCS (Rice and Caniato 2003), thinking that their negligence does not make a difference in the big picture. And even if the negligence made a difference, the managers would reason, their companies would bear only partly the risk of the heightened terrorism. This is why profit-oriented companies tend to underinvest in the counter-terrorism SCS from the society's point of view (Prokop 2012; Bakshi and Gans 2010). To incentivize companies to invest more in SCS, governments have introduced voluntary security-centric AEO programs like the C-TPAT and the EU AEO-S. In essence of the AEO programs is that the customs facilitate traffic of companies that comply with minimum SCS standards. Alas, the companies have an incentive to shirk from the agreed security standards whenever benefits outweigh costs. Due to this opportunistic behavior, the incentive programs run into a risk of moral hazard[41], especially in the absence of adequate enforcement and sanctioning mechanisms that would discourage companies from neglecting their responsibilities. Furher, companies themselves face the risk of moral hazard when they try to incentivize their suppliers and employees to conform to their own supply chain security standards.

Given the conflicting interests, there is a need to reach a mutually satisfying agreement on the type of the SCS collaboration by decising how risks, costs, and benefits of security investments are shared across supply chain partners and government agencies. Academics have suggested a

[41] The moral hazard refers to an actor's readiness take more risk because the risk taker bears only partly the consequences of the downside of the risk outcome.

large variety of incentive mechanisms to align interests and encourage compliance. Joossens and Raw (2008) propose formal agreements, the threat of substantial sanctions, and credible enforcement to make companies to comply governmental anti-smuggling regulations. Bakshi and Gans (2010) advise authorities to set of a credible auditing program to enforce C-TPAT compliance of US companies that, according to their game theoretical analysis, have the interest to shirk from their security responsibilities. The study of Lee et al. (2011) suggests contractual penalties for mitigating slacking of other supply chain partners from security duties. Ideally, the auditing and enforcement activities should be conducted at regular intervals so that there would be a strong incentive for companies to perform consistently at a high level (Bakshi and Gans 2010). The auditing scheme would also ideally involve a random element, a threat of surprise extra audit, so that the companies would not shirk from their responsibilities between scheduled audits. But altogether, the scholars seem to agree that incentive systems should be always devised cautiously, paying close attention to benefits and disadvantages of different coercive and non-coercive incentive mechanisms. In particular, the scholars point out, governments should avoid imposing coercive SCS regulations on companies when other incentive options are available. The problem with regulations is, the scholars argue, that they often disrupt existing business processes and sometimes direct managerial attention from serious security problems to less significant compliance matters.

Many academic studies tout the importance of a strong security culture in pursuing SCS excellence (Williams et al. 2009b; Autry and Bobbit 2008). Practitioners Rice and Caniato (2003) advocate this view by arguing that security should be entrenched into the organization through "socialization," so that the employees would consider security in every-day operations and decision-making. There is a broad consensus that the way users feel about and think of a SCS strategy determines to a great extent how successful the strategy is going to be (Haelterman 2009). Are the users committed to security solution? Do they believe in its effectiveness? Are they aware of the purpose of the solution? Belzer and Swan (2011) suggest that organizations can encourage employees to take their security responsibilities seriously and to stay vigilant to suspicious activities by paying the employees higher salaries that are "above the market clearing price" and by avoiding hiring temporal workforce that might feel alienated from the company values and its security goals. To conclude this sub-section, Table 16 summarizes the design principles on the theme collaboration & culture.

Design principle	Main literature evidence
Devise incentive system using coercive and rewarding incentive mechanisms	Joossens and Raw (2008), Lee et al. (2011), Bakshi and Gans (2010), Voss et al. (2009b)

Regulate cautiously	Prokop (2012), Bakshi and Gans (2010), Reilly et al. (2012)
Pay attention to compensation, hiring, and training	Belzer and Swan (2011), Autry and Bobbit (2008); Voss et al. (2009b), Martens et al. (2011)

Table 16 Collaboration & culture: design principles and evidence

The difficulty to justify SCS spending is another reason why the industry tends to underinvest in counter-terrorism SCS from the society's perspective. Costs of SCS investments are often readily quantifiable while the benefits are uncertain, hard to measure, and tend to accrue over a long time (Whipple et al. 2009; Hameri and Hintsa 2009). For example, security guarding might cost a company 5000 € every month, a significant amount of money that managers could otherwise allocate elsewhere for higher profit or at lower risk. At the same time, benefits of the guarding are unclear. The paradox is that the guarding might have prevented a major terrorist attack or a cargo theft, but nobody knows that because the attack never happened because of the very reason that the guarding was in place (Rice and Spayd 2006).[42] No doubt, managers are having hard time justifying any counter-terrorism investments. And even if managers succeed to negotiate funding for an initiative, they have later no means to demonstrate its payback. The possible positive and negative side effects – collateral benefits (Rice and Spay 2005) or reverse effects (Haelterman 2011) – of preventive SCS initiatives confuse further the investment decisions.

Box 5 Difficulty to justify supply chain security investments

3.5. Research agenda

This section discusses gaps in the contemporary academic SCS research and suggests constructive avenues for future research. The discussion is built on the findings of the literature synthesis.

3.5.1. Explore neglected yet important research topics

The literature synthesis review found that the emphasis of the post-2001 SCS research has been mainly on the maritime logistics and the counterterrorism. This finding was somewhat expected considering that ships carry around 80% of international freight volumes (by weight) and that the sea container logistics has been under ongoing security reform over the past decace (most notable the ISPS code to the US 100% screening act). But unexpectedly, we found also that no studies have addressed air cargo security. This finding is astonishing because air cargo is not

[42] The article of Repenning and Sternman (2001) "Nobody ever gets credit for fixing a problem that never happened" discusses in detail the problems managers face when they try to justify investments in measures that aim to avoid probable costs.

only vulnerable to terrorist bombing plots but also to theft, because of the relatively high value-to-weight ratio of many air cargo shipments. Since the Yemen bomb plot in October 2010, when terorists managed to get two explosive devices onboard passenger planes, civil aviation authorities, the airline industry, and air cargo shippers have been busy designing and implementing more stringent security systems. The practitioners would definitely benefit academic research on, for instance, effects of the EU's ACC3 regulation on cargo handling efficiency and speed, detection accuracy of new screening technologies, and tangible business benefits of Known Consignor and Account Consignor certificates.

Another key future area of the SCS research is cyber crime. Supply chain professionals consider cyber crime as the top-one future crime menace for the logistics industry, as evidenced by a delphi study (PWC 2011) and the managerial accounts collected for this doctoral research. The cyber crime concerns seem warranted given that the global cyber crime seems to be on the rise (UNOCD 2010) and given that the progressing digitalization of logistics information is making supply chains increasingly reliant on computerized systems. But although cyber crime has attracted wide practitioners' interests over the past years, and all signs indicate that the interest continues to grow in the future, the mounting interest has not yet translated into academic research in this topical area, except for a few early explorative studies (Gordon and Ford 2006; Urciuoli et al. 2013). Therefore, the connection between the supply chain and cyber crime merits further investigation, for instance on how cyber crime facilitates main supply chain crimes, such as theft, smuggling, and direct attacks.

3.5.2. Tap into new data sources

Many interesting lines of research remain blocked due to limited access to research data. The main problem is that few companies compile security-related data systematically and even fewer are willing to share this confidential and/or sensitive data with researchers. The companies might consider that revealing data about crime incidents would give a poor impression of their security management, thus giving insurance agencies an excuse to raise insurance premiums or business partners a reason to pressure them to implement new security investments, or authorities a pretext to step up cargo inspections. In the worst case, crime incident statistics would help criminals and terrorists to identify vulnerable targets. Altogether, the lack of reliable statistical data partly explains why many studies have used mainly perceptional measures to gauge the SCS performance (e.g., Voss et al. 2009a; Yang and Wei 2013; Speier et al. 2011; Martens et al. 2011). The problem is that managerial perceptions are subject to many cognitive biases, such as wishful thinking and emphasis on more recent incidents at the expense of older ones. Certainly, numerical incident data has its own flaws and biases, but my suggestion is that researchers would make more effort to locate and negotiate access to business and government databases. I encourage researchers to overcome problems

arising from the data confidentiality by building trusted relationships with key government agencies and companies, fostering best ethical and data privacy practices, and conducting aggregate analyses that allow researchers to mask identities of single data sources. The access to "hard" data would complement the perceptional, qualitative evidence, and enable the researchers to use mixed methods for more credible research. Good news are that the digitalization of the international logistics information proceeds further, so there should be more digital data available in the future.

Besides the business and the government data, SCS research, which has mainly focused on companies, could study more criminals – the antagonists behind the security problems. Future research could investigate the criminals' decisions making processes and try to understand how the criminals plan and execute their crimes. Data for such research could be generated through interviews with convicted criminals or through systematic reviews of court records. Moreover, also the view of government agencies – customs, police authorities, and transport security authorities – could be studied in more detail in the future.

3.5.3. More longitudinal research

After more than a decade of active SCS research, the academic research offers little evidence on whether and to what extent SCS implementation affects the logistics and security performance. This major weakness of the extant literature stems from the lack of longitudinal studies. The vast majority of the earlier SCS studies have cross-sectional research designs, so they cannot say anything about the strength or the direction of cause-effect relationships. For example, even if evidence implied that the SCS performance is positively associated with strategic commitment on the SCS implementation (Voss et al. 2009a), we would not know whether the commitment leads to the performance or the performance leads to the commitment or if there is a third factor explaining the association. Thus, to study causes of security and logistics excellence, I call for more longitudinal research that would measure the logistics performance and the security performance before and after the SCS implementation. The longitudinal research would be important to clarify debated long-term effects security strategies (e.g, Rice and Spayd 2005; Hameri and Hintsa 2009) and to answer the calls for studies focusing on implementation of supply chain risk management strategies (Manuj and Mentzer 2008).

3.5.4. More case study research

There are some strong arguments that highlight the importance of the case study research in the SCS context. First, literature suggests that effectiveness of crime prevention solutions is sensitive to contextual factors (Clarke and Eck 2003) and that the preventive solutions tend to backfire and lead to more violent, frequent, or damaging crime if not properly designed ex ante

(Haelterman 2009). Case studies can offer "thick" contextual descriptions (Eisenhardt 1987) that help us understand why particular security measures succeed or fail in a certain setting. The case study research lends itself well to the longitudinal research, and as noted earlier, the longitudinal research is the only way to get empirical evidence about the causal effects of the SCS implementation to the security and logistics performance. Because multi-case designs bring more compelling evidence than single case studies, especially when the replication logic is used to conduct commensurate case studies (Yin 2009), the multi-case study design should be the standard in the discipline like SCS, which is leaving its fledging years behind and moving from the explolatory phase towards more explanatory and predictive research endeavours. The replicative case studies would also alleviate the problem of generalizability that arises from the single-case research design in general. To conclude this section, I summarize the main points of the research agenda as follows:

- More research on neglected but increasingly important research areas, such as air cargo security and cyber security.
- More research with statistical security data to reduce the current reliance on the subjective data and on the relatively biased proxy measures of the SCS performance.
- More research studying SCS from the perspectives of the criminals and the terrorists as well as the government agencies.
- More longitudinal research to better understand the strength and the direction of cause-effect relationships.
- More case-based research to capture contextual nuances that have consequential effects on the SCS implementation.

3.6. Logistics-friendly SCS management model

This concluding section summarizes the key findings of the literature synthesis by briefly restating the design principles logistics-friendly SCS management and providing illustrative examples how these principles could be applied in practice. Table 17 in the end of this section displays the complete model of logistics-friendly SCS management, with its five themes and associated design principles.

I found that the *mix of security solutions* is highly consequential to the security and logistics performance. Many security solutions seem to function more effectively together than separately. For example, productivity of a team of guards can be increased tremendously with camera surveillance and alarm systems that allow the guards to oversee a large area remotely. Besides the synergies, we observed that the respective sequence of security solutions seems to matter: a combination of a fast primary screening and a more thorough yet slower secondary

screening alleviates system congestion without compromising security. Also a multi-threat primary screening and a subsequent specialized single-threat screening seemed to provide the best results in terms of security and logistics performance. The sequence was also closely associated with alarm thresholds that determine whether shipments should be subjected to follow-up screening. The alarm thresholds can be adjusted to change security level (rate of false positives) and influence system congestion (length of control queue). The literature also proposed that so-called risk-based security implementation is the most-effective way to secure the supply chain. The idea is to assess risk levels of different supply chain entities – shipments, companies, logistics facilities, shipping routes, and so forth – and secure each entity with security measures that are proportional to their risk level. As a rule of thumb, the more granular the risk-based implementation, the more cost-effective is the allocation of security resources. For instance, it is better to assess risk levels of individual shipments than entire consignments of multiple shipments because if a consignment is flagged high risk, every shipment in the consignment must be examined even though risk level of most individual shipments might be significantly lower the risk level of the overall consignment.

The *logistics integration* is about synchronizing security activities into the sequence of baseline logistics process with least disruption to routine logistics. The literature suggests following principles for the logistics integration. First, there is need to identify and eliminate redundant security procedures that contribute little or not at all to SCS performance. We observed that especially unharmonized regulatory regimes create redundant controls (e.g., re-screening of air cargo at origin and every transfer location). If we were not able to eliminate security controls, another possibility is to eliminate associated non-value adding logistics activities (e.g., search of a shipment, moving it to a screening site and back, and so forth). Second, another timesaving design principle is to try to conduct security tasks in parallel with logistics or other security tasks that need to be carried out anyways (e.g., conduct customs, veterinary, and other possible border controls simultaneously). Third, the literature also suggests substituting time-consuming and resource-intensive cargo screening with less disruptive / costly security measures (e.g., use of in-transit monitoring and protection to avoid screening at destination). Fourth, it is important to make sure that security procedures and associated supportive activities (e.g., waiting, preparation, processing) take as little time as possible.

The speed (and the congestion) of the logistics system is closely associated with *the capacity and intensity* of security activities. The more intense the security controls are, the more traffic goes through the security controls, and the faster is the desired speed of the logistics, the higher the capacity requirement of a security system becomes. A sound design principle is to make sure that capacity of a security system can be rapidly expanded if security level were raised

(implying more time-consuming controls), traffic volume increased, or logistics speed requirement were heightened. Also the security system should have a modular design that would allow integration of new sensors and equipment whenever new threats emerged (e.g., new type of synthetic drug or plastic explosive). Another good way to meet security and speed goals is to develop mobile security capabilities that could be deployed rapidly whenever and wherever need for extra capacity arose.

Practices of sharing *security-related information* seem to affect security and logistics performance. We found that logistics operators would benefit a great deal if customs and other government agencies shared their security control principles with the industry. For example, knowing the average and maximum durations of the controls or the likelihood of facing the controls would help the trading community plan post-control follow-up logistics. However, it was also found important to randomize the controls to a degree so that criminals or terrorists could not find foolproof ways to beat the controls. Another information-related finding was the need of lowering the anonymity of the users of the logistics service, shippers and consignees in particular. The lower anonymity would increase the risk of getting responsible for illegal use of the logistics service (e.g., drug smuggling), and thus discourage the criminals from misusing the service.

Collaboration and security culture were identified as important factors of the security and logistics performance. Fundamentally, the collaboration and the culture are means to engage other people and organizations, that do not have otherwise sufficient interest to contribute to SCS management, to take part in the fight against supply chain crime. There are many ways to influence others and make them collaborate. Coercive measures – formal agreements, credible enforcement, and substantial sanctions work in circumstances – work sometimes when the risk of a moral hazard arises (e.g., in cases when it is profitable for a company to shirk from security duties). Sometimes rewarding measures, such as subsidies, privileges, or bonuses, bring better results. The right set of incentives should be determined case-by-case, and decision makers should pay a great deal of attention on this matter. As long as non-coercive measures bring desired results, the literature synthesis suggests that there is no need for regulations. In fact, due to possible negative effects of the binding rules on the logistics and security performance, government agencies should regulate cautiously, only when other options seem inefficient and/or insufficient. We also found that organizations in general should consider their human resource management policies from the security perspective. Security-aware hiring, compensation, and training policies would support building and maintenance of a strong security culture that is characterized by vigilant, skilled, and motivated employees.

Theme and "maxim"	Design principles
Mix of solutions "Security system shall comprise a set of solutions that best meet defenders goals with least resource investments."	• Look for complementary security solutions that provide synergies • Consider sequence of security solutions • Adjust alarm thresholds dynamically to meet desired security level and to cope with system congestion • Pursue risk-based security implementation
Logistics integration "Security solutions shall be integrated into the sequence of baseline logistics activities with least possible disruptions routine operations."	• Eliminate redundant security solutions and associated supportive logistics activities • Process security and logistics activities in parallel whenever possible • Accelerate process time of and queuing time to security processes • Consider substituting cargo screening for other security solutions (e.g., track & trace)
Capacity & intensity "Security systems shall rapidly accommodate to different traffic volumes, threats, and security levels, and logistics needs."	• Design modular security systems that can be adjusted to address new threats • Design rapidly scalable security systems • Invest in mobile security solutions to alleviate congestions and to build early response capability
Secrecy of information "Security information shall be disclosed sparingly, aware of possible benefits and disadvantages."	• Share general information about security principles (e.g., max durations of inspections) • Randomize and alternate security controls to a degree • Reduce anonymity of logistics services
Collaboration & culture "One shall find ways to incentivize others to engage in supply chain security."	• Devise incentive system using coercive and rewarding incentive mechanisms • Regulate cautiously • Pay attention to compensation, hiring, and training

Table 17 Themes and design principles of logistics-friendly supply chain security management

The design principles are strongly rooted in the SCS literature, and they apparently present the "best evidence" the scholarly literature can offer. Even so, practitioners applying the design principles should exercise reasonable caution and consider the design principles only as one input in their decision making process. After all, the design principles are based on rather

divergent theoretical arguments and not so much on consistent empirical evidence. The literature also reminds us that effects of SCS solutions tend to vary significantly from context to another (Haelterman 2009). This observation suggests that there are no universally "optimal" solutions for logistics friendly SCS management, and the design principles proposed here are merely guidance to the right direction.

Summary

This chapter described and synthetized the peer-reviewed academic literature on supply chain security that has been published since 2001. We found that SCS has attracted cross-disciplinary and steadily growing academic interest since 2001. Increasing number and quality studies have established SCS as a standalone discipline that fosters its distinct themes, including sea container screening, protection of cargo from theft and tampering, building security culture, and systematic selection of SCS solutions among multiple options. To address gaps in the current SCS knowledge found in the synthesis, we outlined an agenda for future SCS research. We also learned that there are no universal optimal rules for SCS management, but the literature synthesis revealed some general principles that seem to matter when designing logistics-friendly security systems. Among other principles, it is crucial where security controls are located in the end-to-end supply chain and how they are integrated into the sequence of logistics activities. Also crucial is to strike a balance between secrecy and openness of security information, ensure sufficient capacity of security controls, build security culture, and engage in business-to-business and business-to-government collaboration.

Chapter 4 | Supply Chain Crime Taxonomy

This chapter starts with a brief review of the academic literature to identify key characteristics of supply chain security (SCS) risks. Building on this characterization, the chapter analyzes managerial perceptions on crime problems that occur or could occur in the supply chain context. These managerial views on the supply chain crime problems are then used to develop a taxonomy of supply chain crime. The chapter proceeds to discuss theoretical and practical implications of the supply chain crime taxonomy. The chapter concludes by assessing the validity of the taxonomy by applying it to the context of the Swiss-centric international postal logistics.

4.1. Supply chain security risks

Since the 9/11 attacks in 2001, academics have been producing studies on supply chain security (SCS) in increasing numbers. Today, more than a decade after the early years of SCS research, the academic community seems to have reached some degree of agreement on defining characteristics of the risks that SCS management addresses. The dominant academic view is that security risks in the supply chain context stem from man-made, illegal activities. Many scholars characterize such illegal activities as intentional crimes, committed by conscious actors for a purpose (Williams et al. 2009a; Sheffi 2005; Ekwall 2009a; Martens et al. 2011). Some academics, however, hold cautiously a mixed view and argue that security risks may occur also due to unintentional human errors or negligence (Speier et al. 2011). However, the most disputed characteristic of the supply chain security risk is related to its effect on business logistics. One stream of the academic literature suggests that security risks are inherently detrimental to supply chain operations (e.g., Ekwall 2009a; Lee et al. 2011). This view mirrors the general understanding of supply chain risk as something that may result only in undesirable consequences (Peck 2006). Granted that because SCS risks arise from criminal activity and crime is always undesirable from the law enforcement perspective. But this is not always the case when considering crime from the business perspective. Consider, for example, smuggling in fake counterfeited apparels. As long as customs or other law enforcement agencies do not delay routine logistics due to smuggling investigations or seizures, it is hard to argue why illegal traffic in fake soccer shirts would be detrimental to the business operations. In fact, in the big

picture, logistics service provider *benefit* from smuggling as long as the smugglers pay shipping fees like law-abiding customers.

Based on the earlier literature, we can conclude so far that supply chain security risks stem from intentional man-made criminal activities that might be detrimental to logistics. Alas, this definition hinges on two elusive concepts: supply chain and crime. The both concepts call for clarification. A supply chain, Waters (2003) suggests, "consists of the series of activities and organizations that materials move through on their journey from initial suppliers to final customers." Peck (2006) refines the supply chain concept further by arguing that supply chains are networks (rather than chains) of interconnected and interdependent organizations involved in a sequence of production and distribution related value-adding processes. She continues, building on earlier scholarly literature, that the supply chains are conduits for inter-organizational exchange of goods and materials and that the supply chains are underpinned by logistics and communication infrastructure. In turn, crime can be defined as an act, or an omission of an act, that the government has prohibited and may thus lead to state-administered sanctions (Farr and Gibbons 1990)[43]. By definition, crime is illegal, and the illegality is defined by the law. But despite the apparent definitional clarity, it is problematic to define crime in the supply chain context because global supply chains span many countries and each country tends to respect their idiosyncratic bodies of national laws. Given the national differences, we cannot establish a universal law-based definition for supply chain crime. Instead, in this thesis, I define crime as an act that supply chain practitioners collectively, but not necessarily unanimously, consider illegal. This intersubjective definition allows us to assume that theft, smuggling, document fraud, sabotage and terrorism, for example, are criminal acts although some bodies of national legislation might not recognize these crime concepts or consider them as crime. To conclude this introductory section, Table 18 presents some key academic definitions of risks that SCS management addresses.

Article	Risks addressed by supply chain security management
Williams et al. (2009a)	"Damage, terrorism, and contraband […] to prevent man-made supply chain disasters."
Speier et al. (2011)	"Contamination, damage, or destruction of products and/or supply chain assets"
Ekwall (2009a)	"Deliberately caused illegal and hostile threats against the planned or wanted logistics process, function, and structure"

[43] In this dissertation, I do not make make a difference between offences that violate the criminal code and offences that count as administrative violations. Nevertheless, I acknowledge that further analysis of legal technicalities on this matter is an important area for future research.

Manuj and Mentzer (2008)	"Freight breaches, terrorism, vandalism, crime, and sabotage"
Closs and McGarrel (2004)	Theft, damage, or terrorism, and […] the introduction of unauthorized contraband, people, or weapons of mass destruction in the supply chain."
Sarathy (2006)	"Terrorist and security threats"
Pfohl et al. (2010)	"Attacks and disturbance with a criminal intent"

Table 18 Academic views on supply chain security risks

4.2. Managerial perceptions on supply chain crime

This section presents supply chain crime themes that managers consider important. The subsequent analysis is based on perceptions of 18 managers my colleagues and me have interviewed / surveyed for this study. Readers seeking for further details about the data collection and the data analysis are advised to consult in chapter 2.

4.2.1. Theft of cargo and vehicles

Cargo theft was one of the most commonly mentioned crime problems among the interviewed managers. Theft of goods (and vehicles) seemed to be particularly important concern for managers who deal with manufacturing, shipping, and sales of high-value goods such as pharmaceuticals and electronics. Although in principle cargo is at risk always and everywhere in the supply chain, the managers told that most theft incidents in their supply chains occur during road and air transportation. We learned that thieves tend to attack when cargo is in transit, outside protective walls of warehouses, ports, and other logistics facilities. In-transit truckloads are particularly vulnerable when the trucks are stationary and left unattended, for example during overnight stopovers or during ferry transport. Regarding modi operandi, armed robberies, hijacks, and other violent methods of stealing cargo and vehicles concerned the managers most. The employee safety is a reason why a pharmaceutical company, for example, instructs drivers not to resist when threatened with violence, regardless the high value of the cargo they transport. Besides resorting to violence and intimidation, the cargo thieves often use deceptive methods to hijack loads. The thieves might set up a front company or abuse identity of a reputable carrier company to pick up loads from unexpected shippers, straight from their factories and warehouses, but never deliver the cargo to the indented destination. Aside the audacious attitude, the managers pointed out, forged, altered, or dishonestly acquired drivers' IDs, bills of ladings, and other documents often facilitate the deceptive pick-ups. Another key facilitator of cargo theft is confidential logistics information (e.g., contents, scheduling, and routing of shipments), which enables especially professional cargo theft rings, which operate on steal-to-order basis, to identify desired targets. The managers told me that the

thieves could obtain for the confidential information for example from company insiders, through cyber crime, or by systematic visual observations. One manager also blamed customs officers for disclosing information that lead to theft of a shipment of 200 drums of printing ink.

4.2.2. Terrorist threat

Besides cargo theft, managers were commonly concerned about the possibility that terrorists or other hostile agents would attack their supply chains or exploit the supply chains to attack third parties. The risk of terrorism appeared to be particularly high in the airfreight channel where a single explosive device, if accidentally loaded on board among airfreight, could blast air freighters and passenger planes into pieces. Logistics service providers raised concerns of the risk of terrorists hijacking ships, trucks, and planes and their (hazardous) loads using them as weapons for destruction, much the same way than in the infamous "9/11" attacks. It was also mentioned that the terrorists could try to contaminate food, pharmaceuticals, and other consumables to spread terror among the general population. However, perhaps the most alarming terrorist and criminal trend is related to the information and communication technologies (ICT), on which modern supply chain worldwide are increasingly dependent. One of the respondents, for instance, indicated that the terrorists could use cyber crime techniques to interfere with avionics systems with dire consequences of messing up air traffic. Another manager assumed that cyber crime techniques could make criminals and terrorists more capable of stealing sensitive logistics and security information from electronic databases. The sensitive information in turn would help the antagonists to circumvent existing security system and thus facilitate sabotage and criminal exploitation of the supply chain.

4.2.3. Smuggling through the supply chain

The managers noted that criminals might hide contraband among legitimate cargo and inside vehicle structures, with intent to evade borders controls. The managers were mainly concerned about bombs and contaminants entering the supply chain, but also unathorized introduction of narcotics, counterfeits, and contraband tobacco raised concerns[44]. Like in the case of cargo theft, the risk of tampering was considered particularly high when goods are in transit, standstill, and unprotected. The managers also assumed that the criminals use corruption, document fraud, and identity theft to get their contraband into the supply chain and to facilitate illegal movements across national borders all the way to the target markets. A key business reason for fighting (non-dangerous) contraband was to keep border control authorities satisfied and thereby avoid fines, revocations and suspensions of licences, and frequent and time-consuming

[44] It should be noted, however, that the range of illegal goods, which may enter the supply chain, is much wider.

inspections that might follow if authorities found undeclared commodities among the legitimate cargo. Interstingly, a few managers also indicated that sometimes undesired commodities enter the supply chain due to dishonest activities of their business partners. In one incident, an Asian supplier falsified product certificates, by stating that the working life of a light bulb was around 10.000 hours, when in fact, it was only 5.000 hours. In another slightly different case, a company employed to dispose expired medicines decided to channel the outdated pharmaceuticals to back to (black)markets. A similar product diversions fraud, experienced by an electronics company, involved a Russian wholesaler which sold electronics outside the contracted Russian market to get higher margin for the products. Table 19 below summarises crime themes that my collegues and me identified in the interview data.

Crime themes	Definition by authors
Bogus companies	Use of bogus or otherwise legitimate front company for crime.
Corruption	"Abuse of entrusted power for private gain." (Transparency International 2012)
Counterfeiting	Production, distribution or sales of goods that violate intellectual property rights.
Cyber crime	Use of ICT technology to steal information or sabotage supply chains.
Document fraud	Use of forged, altered or dishonestly acquired electronic or paper-based documents.
Insider fraud	Crimes committed by an employee against his/her employer.
Product diversion fraud	Distribution or sales of legitimate goods outside of contracted markets and sales channels.
Product specification fraud	Deceptive sales of materials or products that do not comply with contracted specifications.
Sabotage	Intentional harming / damaging of people, property, information and infrastructure.
Smuggling	Illegal movement of goods into or out of a country.
Terrorism	Use of intimidation or violence to attain political or ideological objectives.
Theft	Theft of goods and/or vehicles by force or deception.
Use of violence	Intimidation, assault or abduction of an employer.

Table 19 Crime themes and definitions

4.3. Supply chain crime taxonomy

The views of the 18 managers illustrate a broad diversity of criminal activities that take place in the supply chain context. The most prominent crime themes seem to be terrorism, cyber crime, smuggling, and cargo theft in many forms (e.g., robbery, hijack, and product diversion). The themes of violence and deception also recur throughout the managerial accounts. These themes lend support to the observation that supply chain security risks stem from illegal and intentional man-made activities that may cause problem to logistics management. But more importantly, further analysis reveals that the criminals intervene with the supply chain three main ways: 1) by removing assets out of the supply chain, 2) by introducing contraband into the supply chain, 3) and by attacking supply chains directly. Besides, a range of supporting criminal methods and means facilitates the criminals to intervene with the supply chain. The three ways of criminal interaction and the observation, that the criminals often facilitate their activities by other illegal means, set the basis for the supply chain taxonomy I describe next.

4.3.1. Theft class

The first taxonomic class encompasses crimes in which criminals remove assets from the supply chain without authorization. By assets I mean mainly cargo and vehicles, though technically the criminals could also loot factories for machinery or abduct people for ransoms (e.g., sea pirates capturing a ship and its crew). I call this first taxonomic group as *theft* class, deeming that such a general name captures best the wide array of crimes that involve stealing (or unauthorized removal of assets to be more precise). Crime types falling into the *theft* class include robbery (taking by force or intimidation), hijacking (capturing of vehicles in transit), burglary (stealing by intrusion), deceptive pickups (stealing by pretending to be someone else), and sea piracy (robbing ships at sea). The *theft* class also covers activities called organized cargo theft and pilferage, which draw attention to the scope of activity and the character of the thieves themselves.

4.3.2. Smuggling class

The second taxonomic class, called *smuggling*, comprises crimes involving people who introduce contraband or security threats into the supply chain. The security threats refer to chemical, biological, radiological, and nuclear weapons and explosive devices – commonly abbreviated as CBRNe threats. The security threats have potential to kill, maim, or otherwise cause damage while they travel through the supply chain. Contraband encompasses five general types of illegal commodities. The first three "trade-control" contraband types are labelled as absolute, relative, and fiscal. The absolute contraband consists of inherently illegal

commodities such as stolen goods, counterfeits, and illegal drugs, which importation, exportation, or possession is forbidden under any circumstances. This is different from the relative contraband that covers a wide array of otherwise legal goods that become illegal when they cross borders without appropriate permits, licenses, certificates, or other authorizing documents. The fiscal contraband refer to the otherwise legal commodities that are imported / exported without paying appropriate duties and taxes. Besides the trade-control contraband, we can distinguish safety contraband that is transported without paying regard to regulations governing safe transport of goods (e.g., fireworks, matches, or sulfur acid). The fifth contraband type, contractual contraband, includes merchandise that violates contractual requirements unilaterally and deceitfully (e.g., goods produced with child labor, sold outside agreed markets, or not meeting safety standards). Table 20 summarizes the general types of contraband and active weapons and provides examples.

Type of illegal goods	Description	Violates	Example commodities
Absolute contraband*	Commodities not allowed for export/ import and which possession might be illegal	Prohibitions	Narcotics, stolen goods, counterfeits and sub-standard consumer goods
Relative contraband*	Commodities exported/ imported without authorization	Trade restrictions	Firearms, pharmaceuticals, and hazardous waste
Fiscal contraband*	Commodities exported/ imported without paying appropriate duties & taxes	Tax & duty laws	Cigarettes, alcohol, and fuels
Safety contraband	Prohibited or inadequately packed / marked / handled dangerous goods	Dangerous goods transport regulations	Sprays and aerosols
Contractual contraband	Goods intended to pass as quality one even not meeting contractual requirements	Business contracts	Products not meeting contractual requirements, parallel traded goods
CBRNe weapons	Devices or substances introduced to supply chains with intent to damage, injure, or kill	Dangerous goods transport regulations & prohibitions	Chemical, biological, radiological, and nuclear weapons; improvised explosive and incendiary devices*

Table 20 Types of contraband and security threats (*adapted from Naylor 2003)

The types of contraband overlap to a degree, as Figure 7 illustrates. Untaxed cigarettes and heroin are pure examples of fiscal (1) and absolute (2) contraband, respectively. Undeclared doping substances match the description of both fiscal and relative contraband (3). Stolen hand grenades count as absolute and hazardous contraband (4). Undeclared fireworks break fiscal laws, licensing requirements and dangerous goods regulations and are thus fiscal, absolute and hazardous contraband at the same time (5). Improvised explosive devices (IED) are absolute, malicious and hazardous contraband (6). A shipment of undeclared and poorly packaged cigarette lighters counts as purely hazardous contraband (7). Most illegal or otherwise undesirable contraband articles are also contractual contraband (8).

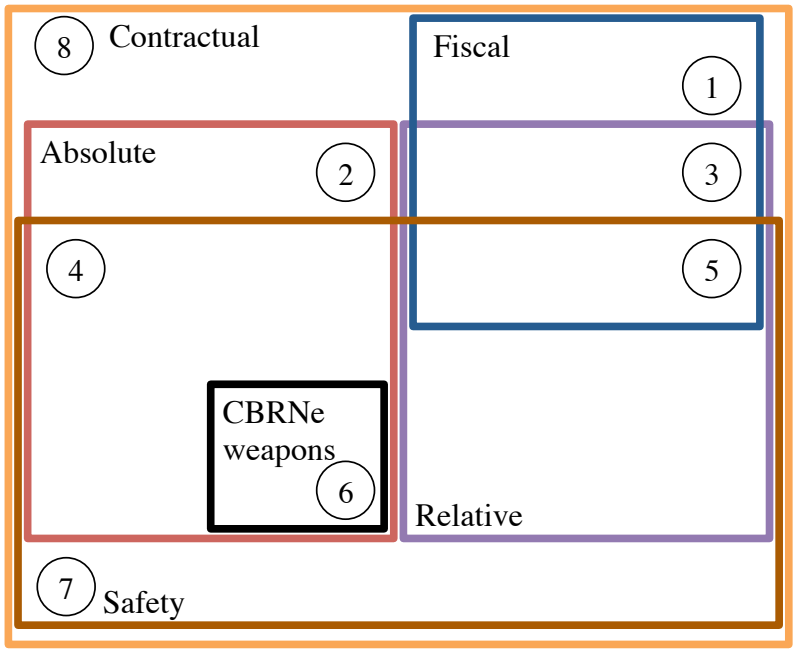


Figure 7 Overlapping types of contraband and security threats

Contraband and weapons may enter the supply chain two main ways. The first method is to hijack a shipment of a legitimate shipper as it moves through the supply chain: smugglers intercept a shipment somewhere along the route, open it, and insert illegal goods inside, before resealing and letting the shipment to continue its journey. The second, the "Trojan horse" method, involves a contraband shipper who pays appropriate shipping fees and behaves like any law-abiding user of logistics services (OECD 2005). A Trojan horse shipper would prepare illegal shipment at his own premises before handing it over to a carrier in a routine business transaction. To defraud customs and other law enforcement authorities, the rogue shippers often use false shipping documentation and conceal their unauthorized cargo among legitimate goods. Absolute contraband and CBRNe weapons are smuggled under a false tariff code (i.e.,

HS code). Smugglers of fiscal contraband typically understate value, quantity, or weight of their goods, misclassify the goods as a commodity with lower duty or tax rate, or declare a false country of origin to benefit from prefential duty rates (e.g., zero duty for trade union members). The misclassification and the false declaration of the country of origin also enable smugglers of relative contraband to evade licensing requirements, quotas, anti-dumping duties, and embargoes. The false country of origin is also used to cover up origin of source-sensitive commodities like diamonds, timber, and some minerals (e.g., coltan). Providing false information about the country of destination and the consignee helps exporters evade embargoes and licensing requirements. By exaggerating value of their cargo, the dishonest traders can avoid price floors set by anti-dumping policies as well as inflate export records, thereby "justifying" fradulent claims of VAT refund, export subsidies, or drawbacks. Table 21 summarises methods smugglers use to deceive border control agencies. Box 6 explains how different stakeholders lose money due to the tax and duty evasion.

Illegal commodity:	Absolute & CBRNe	Relative				Fiscal
Violation of: / Modus operandi	Prohibitions	Licensing requirements	Quotas	Anti-dumping policies	Embargoes	Tax & duty rules
Undervaluation						X
Overvaluation				X		
Underdeclaration of quantity			X			X
Misclassification	X	X	X	X	X	X
False country of origin		X	X	X	X	X
False country of destination		X			X	
False consignee		X			X	

Table 21 Methods of deceiving border controllers

Contraband traffic often results in a loss of tax revenues for governments and lost sales for the companies. Fiscal contraband – commodities transported across borders without paying appropriate duties and taxes – is a major issue for the governments because tax and duty evasion can make a gap in the national budget. The amount of lost taxes and sales revenues is a more complicated with other types of contraband. Governments do not levy duties or taxes on inherently illegal commodities like heroin or cocaine. Therefore, if an undeclared shipment of illegal drug passes the border controls, governments do not lose tax revenues. The case with counterfeits, another variety of inherently illegal absolute contraband, is less clear-cut. Governments lose tax revenues indirectly if the fake products decrease sales of genuine products, which are normally taxed. For each genuine product not sold, companies lose the sales margin and the government VAT and possible excise taxes. The producer's margin and the governments' tax cut depend on the product. If relative contraband were traded according to the law, governments would collect taxes from this trade. So when a load of undeclared handguns crosses borders undetected, the governments lose tax and duty revenues. Later blackmarket sales of small arms reduce demand for lawful firearms, which affects legitimate arms dealers, and reduces taxes the dealers pay.

Box 6 Impact of trafficking on tax and sales revenues

4.3.3. Direct attack class

The *"direct attack"* class covers hostile activities that aim to damage supply chain infrastructure, vehicles, cargo, or people. The direct attacks are immediate, and unlike many crimes in the smuggling class, the direct attacks do not involve something illegal moving through the supply chain. For example, a derailment of a cargo train, a sinking a container ship, or a shoot-down of an airfreighter all count as direct attacks because the attackers strike immediately instantly, and they come from the outside of the supply chain. Other examples of direct attacks include sabotage on air traffic control systems and arsons of warehouses, ports, or other logistics facilities.

4.3.4. Crime facilitation class

The *"facilitation"* class entails supporting crimes that help criminals commit theft, smuggling, and direct attacks – the above described primary supply chain crimes. The supporting crimes do not bring direct reward for the criminals, but they provide means and methods for pursuing the rewarding primary crimes. We can identify six facilitating crimes based on the managerial descriptions of the crime problems: identity theft, corruption, cyber crime, insider fraud, document fraud, and use of violence and intimidation. Theft of corporate identity of a reputable company (e.g., an AEO holder or a known consignor) helps smugglers infiltrate illegal goods into the supply chain and get them across international borders. Masking illegal activities behind a seemingly legitimate front company also helps cargo thieves to pick-up loads from unexpected shippers. Also, bribing of officials and supply chain insiders smooths the way of

contraband and CBRNe weapons into and through the supply chain[45]. Corrupted or otherwise solicited entrusted officials and business insiders may also collude with cargo thieves. Involvement of the supply chain insiders in crime, either as a facilitator or a perpetrator, poses a unique security risk because the insiders can access to confidential information, tamper security systems, and solicit other employees to crime or negligence. A complicit warehouse worker, for example, might divulge inventory records for burglars, pinpoint exact location of targeted goods inside the warehouse, and purposefully "forget" to lock the backdoor and activate burglar alarms for night. Cyber crime, defined as any activity where ICT technology is an agent, facilitator or target of crime (Gordon and Ford 2006), helps criminals get access to confidential information, take over computer systems (and switch off alarm systems for example), and sell illegal goods online. As said earlier, fraudulent documents help smugglers to deceive border control officials and cargo thieves to pick up loads. Finally, violence and intimidation can be the goal (e.g., direct attack) or facilitator of supply chain crime (e.g., robberies).

To conclude this section, Table 22 below summarizes the four taxonomic classes. The table also matches the four classes with supply chain crime themes that the interviewed managers described.

Taxonomic class	Criminal intervention	Matching crime themes
Theft	Unauthorized removal of assets from the supply chain	Robbery, terrorism, counterfeiting
Smuggling	Introduction of contraband or CBRNe weapons into the supply chain	Terrorism, product specification fraud, counterfeiting, production diversion fraud
Direct attack	Attack on supply chain infrastructure, vehicles, cargo, or people	Terrorism, sabotage, vandalism
Facilitation	Supporting means and methods for committing theft, smuggling, and direct attack	Identity theft, corruption, cyber crime, insider fraud, document fraud, and use of violence and intimidation

Table 22 Classes of supply chain crime taxonomy and matching crime themes

4.4. Discussion

This concluding section discusses first terrorism, counterfeiting, and some other overarching crime phenomena that seem to fit into more than one class of the supply chain crime taxonomy.

[45] Bribing people to turn a blind eye to crime is one variety of corruption. Another variety is to pay people to do the work they should be doing anyways.

The second part of the section explains why the supply chain crime taxonomy is not just an artificial, over-simplified reflection of the reality without any practical relevance.

4.4.1. Overarching crime themes

Certain crime themes match multiple taxonomic classes. Terrorism is perhaps the most striking example. The concept of terrorism refers generally to the use of intimidation and violence in pursuit of idelogical goals. When the use of violence is particularly destructive, or the motive for attacking is obviously political, the general public usually talks about terrorism, otherwise sabotage. Because of this wide definition, terrorism covers a variety of criminal activities, which are connected to commercial supply chains to a varying degree. Examples of terrorist attacks that take place outside the supply chain context include hijacks of passenger planes, drive-by assassinations, and roadside bombings against military convoys. On the other hand, being a broadly defined concept, terrorism may be connected virtually to any criminal activity occuring in the supply chain context. Certainly, intentional derailment of a cargo train, malicious product tampering, and shipping of biological weapons through the supply chain count often as terrorism. Terrorists could also exploit the supply chain to smuggle people, material, and technology that is needed to organize an attack, for example enriched uranium or nuclear technology. Accordingly, two taxonomic classes, *direct attack* and *smuggling,* are linked to terrorism. But it seems that terrorism can also be associated with the *theft* class, defined by the unauthorized removal of assets from the supply chain. Terrorists could steal a truck load of hazardous cargo and later use the stolen load to mount a devastating attack. They could also hijack a vehicle of transport, let say an oil tanker, a cargo plane, or a freight train, and use the vehicle and its cargo as a weapon against a target. Moreover, the terrorists could fund their hostile activities with money they generate through a variety criminal activities, including cargo theft and smuggling.

Another overarching crime theme is counterfeiting, defined here as production, distribution, or sales of products that violate intellectual property rights (IPR). Sometimes the production of counterfeits takes place at otherwise legitimate manufacturing facilities. A dishonest factory owner, for example, might run a few extra producton shifts, exceed his contracted production quota, and sell the extra output for own profit without informing his client, the IPR-holder. Likewise, business partners towards the downstream supply chain – wholesalers, retailers, or even companies hired to take care of reverse logistics – may disregard business contracts and divert products to unathorized markets, thus turning the otherwise bona fide products into de jure counterfeits. We could interpret such behavior as some kind of theft because of stolen IPR and because the products are removed from the legitimate supply chain without authorization. This interpretation links counterfeiting obviously to the *theft* class of the taxonomy. But

counterfeiting is also associated with the *smuggling* class because fake products often travel to their target markets through the international supply chain.

More generally, we can fight many global criminal phenomena by reducing supply chain crime. Anti-trafficking measures curb smuggling, and thereby decrease illicit trade and its related criminal phenomena, including drug trafficking, nuclear proliferation, counterfeiting, gunrunning, people smuggling, and waste trafficking. Counter-terrorism security mitigates the risk that terrorist would hurt the society by attacking the supply chain itself or by abusing the supply chain to smuggle tools of terrorism. Moreover, fighting cargo theft would make it harder for criminals to acquire goods – pharmaceuticals, brand apparels, works of art and so forth – to be sold at black markets. Combating cross-border trafficking in stolen goods would make fencing more difficult and thus make organized robberies, burglaries, shoplifting and other varieties of property crime less attracting. As rogue online pharmacies ship their merchandise to buyers via express couriers or by post, fighting smuggling would reduce illicit medicine trade but also lower related criminal activities, most notably the procurement of medicines through cargo theft. Moreover, if facilitating crime is a key enabler of primary supply chain crimes, fighting document fraud, identity theft, cyber crime, and other crime facilitators reduce supply chain crime. For instance, biometric driver licenses or forgery-resistant shipping documents would evidently reduce frequency of deceptive pickup attempts. Dismantling online cyber crime gangs would reduce the threat of online-based sabotage and data theft also in the supply chain context.

4.4.2. Further implications of the taxonomy

Various crime types engender supply chain disruptions of different magnitude. Major terrorist attacks, as pointed out earlier, trigger supply chain disruptions that often radiate far beyond the immediate setting of the attack. A direct attack on the supply chain – for example sinking a ship at a major port or at one of the world's maritime gateways (e.g., the channel of Panama) – would no doubt seriously disrupt international transport and logistics. Nevertheless, consequences of one magnitude higher could realize if terrorists sent chemical, biological, nuclear, radioactive, or explosive weapons through the supply chain. A detonation of a nuclear device in a seaport would contaminate large areas useless, result in mass casualties and huge property losses, and lead to introduction of new precautionary security measures throughout the global supply chain. Biological attacks through the supply chain could trigger a worldwide pandemic outbreak, in the worst case. Attacks with conventional bombs and chemical weapons seem less potent risks, but in fact, a series of attacks with relative low yield weapons could paralyze the international logistics (consider a set of bombs in the air cargo channel). Cargo theft may lead to financial and reputational losses and jeopardize work safety (e.g., violent robberies) or consumer safety (e.g., a loss of a time-critical medicine delivery). But unlike the

major terrorist attacks, one or more cargo theft incidents do not grind the entire international logistics into a halt. After all, most theft incidents are minor deviations from logistics plans, so it would be exaggeration to talk about disasters or major disruptions. Contraband smuggling is often even less disruptive to logistics than cargo theft. In fact, trafficking in drugs, counterfeits, or stolen goods does not disrupt the logistics as long as the clandestine traffic goes undetected. The disruptive effects of the contraband smuggling are related to possible time-consuming customs inspections and seizures. It should be noted, however, that undeclared goods might cause supply chain disruptions under unfavorable circumstances. For instance, investigators of the wrecked container ship MSC Napoli in 2007 discovered systematic under-declaration of container weights and ascribed the behavior to shippers' attempts to save in weight-based duties and shipping fees (MAIB 2008). To sum up, it is fortunate that the more disruptive a crime risk is, the less likely it is to happen.

The taxonomic classes also seem to have some differences in terms of what role the supply chain plays in crime. In the contraband smuggling, smugglers exploit the supply chain for their criminal activity. The supply chain, used as a vehicle for crime, does not necessarily get disrupted or face any adverse effects due to the smuggling activity. On the other hand, theft is a predatory crime that clearly victimizes the companies involved in the supply chain. In case of theft, the supply chain is clearly the victim rather than the vehicle of crime. The direct attacks and the smuggling of the CBRNe weapons both victimize the supply chain and it as a vehicle for crime.

The crimes of the taxonomic classes also differ in terms of which stakeholders are interested to address the risks they pose. Theft is a concern mainly for companies, which worry about cargo losses, failed deliveries, and violence involved in theft incidents, especially hijacks and robberies. The law enforcement is certainly responsible for investigating cargo theft, but industry associations like TAPA drive the anti-theft agenda for example by maintaining anti-theft standards, lobbying for secure parking lots and more severe punishments for thieves, and demanding dedicated cargo theft prosecutors. Smuggling in CBRNe weapons and direct attacks are definitely concerns for the companies. However, it is now the authorities that drive the agenda in the counter-terrorism supply chain security by issuing regulations, auditing companies, introducing partnership programs, and enforcing the cross-border traffic. In case of the contraband smuggling, the authorities drive the security agenda almost exclusively[46]: customs and other border control agencies are responsible for collecting taxes and duties (fiscal

[46] Trafficking in counterfeits is the only segment of the overall contraband trade that the business sector is committed to fight, even more than the customs. But interestingly, these concerned companies are not cargo owners (shippers or consignees) or logistics services providers (carriers or freight forwarders) but firms that own the intellectual property of the copied articles.

contraband) from the cross-border traffic as well as enforcing trade in prohibited and restricted commodities (absolute and relative contraband).

The last major difference between the taxonomic classes relate to the cargo integrity. Recall that cargo retains its integrity as long as unauthorized people – thieves, smugglers, and terrorists – cannot tamper with it. Interestingly, the *theft* and the *smuggling* classes involve tampering of cargo: thieves take cargo out, and smugglers put something in. By contrast, crimes in the *direct attack* class originate from the outside of the supply chain, are not connected to the cargo flow, and require no tampering. This observation shows that the cargo integrity is a crucial concept in the supply chain security management: it allows us to fight theft and smuggling simultaneously. Therefore, security solutions that seek to protect and restore the cargo integrity should be the core of any SCS system.

This section elaborated some arguments why the supply chain crime taxonomy is relevant for practical supply chain security management. To sum up this discussion, Figure 8 illustrates differences between the three main classes of supply chain crime taxonomy.

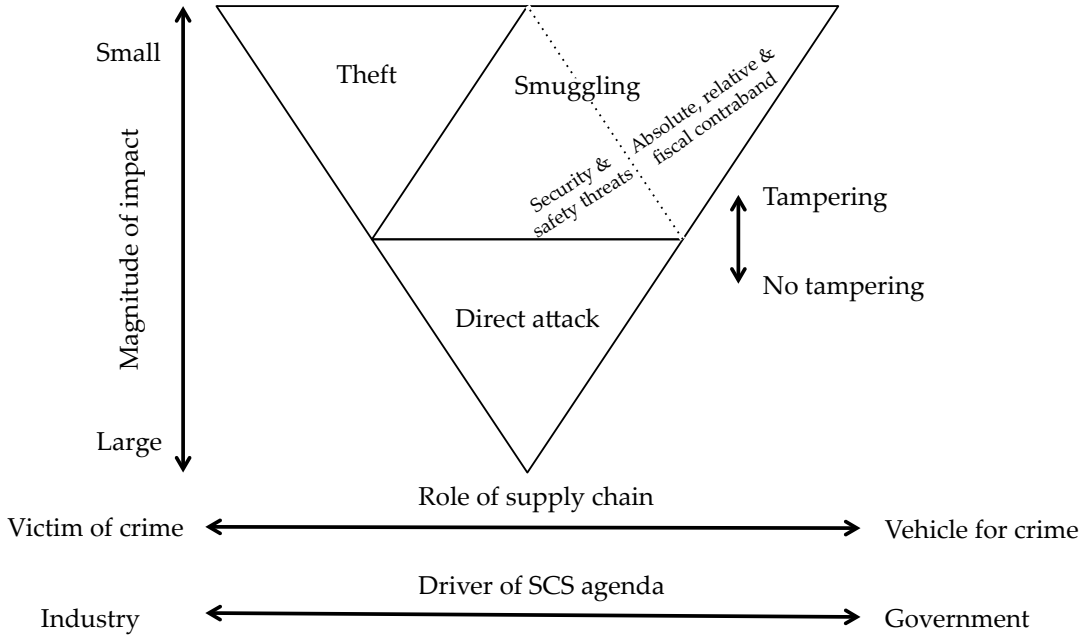


Figure 8 Further differences of the three main taxonomic crime classes

4.4.3. Difference between security and general supply chain risks

The defining characteristics of supply chain security risks allow us to demarcate supply chain security (SCS) from general supply chain risk management (SCRM). But before proceeding into particulars, let us define *risk sources, risk events, and risk consequences*, three components of the overall risk concept that set the foundation for the following discourse. Risk sources are underlying hazards capable of triggering events that result in risk consequences. Examples risk

sources include natural catastrophes, strikes, currency volatility, terrorism, and political turmoil. Most risk sources generate events that can lead to a range of risk consequences, such as late deliveries or lower customer satisfaction. Risk consequences are defined as effects of risk events on objectives[47] (ISO 2009). Therefore, consequences of a singular event depend on observers and their subjective goals. Consider, for instance, consequences arising from a strike that closes seaports. Exporting companies might consider effects of such labour dispute in terms of inability to meet contracted delivery schedules, which may further translate into lower customer satisfaction and worse business performance. But authorities perceive the effect of the same port closure mainly in terms of slower economic growth and problems of importing food, fuels and other critical supplies.

Given that supply chain security risks stem from man-made intentional criminal activities, many types of general supply chain *risk sources* fall out of the scope of supply chain security. Defined as man-made activities, supply chain security risk sources cover natural disasters, technical failures, and other hazards, that trigger risk events without direct human involvement. Moreover, because security risks involve deliberate actors, inadvertent human mistakes have nothing to do with security, even though carelessness and negligence may sometimes lead to criminal charges. Furthermore, under the condition of illegality, legal strikes and labour disputes are not sources of security risks despite being intentional, man-made and potentially disruptive. Altogether, because SCS addresses only a distinct sub-set of all risk sources, which may generate risk events in the supply chain context, SCS can be considered as a subfield of SCRM from the risk source perspective.

But interestingly, when we shift our attention to *risk consequences*, SCS seems to dwarf SCRM, its apparent parent discipline. The two disciplines share the same commercial purpose of safeguarding business continuity and profitability through the management of supply chain risks. But whereas SCRM considers the risk consequences purely from the business position, SCS assumes a broader multi-stakeholder perspective, which involves views of both the business operators and governments. The governments play a more prominent role in SCS than in SCRM because security risks involve criminal activities, and crime is a matter of law enforcement. Another, perhaps more important reason for the government involvement is that the criminal activities in the supply chain context often engender wide social harm that

[47] Risk consequences can affect objectives negatively or positively. The upside potential of risk is clear in fields like finance, project business, and entrepreneurship where uncertainty may result in serendipitous surprises. However, supply chain risk bears typically only the downside connotation, as any deviation from plan would result in undesired consequences in highly synchronized modern logistics networks (Peck 2006).

transcends the business interest. Risk consequences arising from terrorist and trafficking activities, in particular, radiate far beyond the immediate supply chain setting where a security breach occurs. For example, the worldwide air cargo and mail service was seriously disrupted in October 2010 when authorities introduced new security measures after the discovery of two explosive devices on board airplanes during the Yemen terrorist bomb plot. The radiating effects of security breaches are even more obvious in trafficking: smuggling in war material triggers and fuels conflicts, illegal trade in green house gases accelerates global warming, and drug trafficking increases crime and inflates health care expenditures, among other examples. To conclude so far, criminal activities in the supply chains create and exacerbate numerous social problems, many of which are key concerns for various government functions and policy-making areas, including border controls, national security, and public health. This observation and the illegal nature of security risks explain the prominent role of the governments in SCS. Table 23 sums up the key differences between supply chain risk management (SCRM) and supply chain security (SCS).

	Supply chain risk management	Supply chain security
Risk sources	All hazards	Hazards stemming from man-made intentional criminal activities
Risk event	Supply chain disruption	Security breach
Risk consequences	Worse business performance	Worse business performance + wide social ramifications

Table 23 Differences between supply chain risk management and supply chain security

We know now how supply chain security differs from supply chain security risk management. But what remains unanswered is how the differences affect research on and practice of supply chain risk management. Intentionality of criminal activities implies that supply chain security opposes intelligent antagonists, which adjust their behavior in response to security measures. Assuming that the antagonists are rational, which is a judicious assumption when considering professional career criminals, the criminals tend to plot their crimes beforehand and execute them according to a plan. If the antagonists are rational and able to adjust their behavior, we can try to dissuade them from committing crime. The higher is the risk of getting caught and punishmed and the lower is the reward-to-effort ratio, the less willing criminals are to commit crime. Therefore, in supply chain security, we can tap into the traditional field of criminology to understand how to design security and legal systems in a way that enable us best prevent, detect, and investigate crime in the supply chain context. In the previous systematic literature

chapter, I expanded more on key criminological theories that underpin effective management of supply chain security risks.

Managers and academics have realized long ago that collaboration among business partners underpins efficient management of risks in the supply chain. Likewise, managing *security* risks require collaboration among the businesses partners. But given the prominent role of the governments in SCS, collaboration must exist also among government agencies and between the businesses and the government agencies. These three types of collaboration – business-to-business, government-to-government, and business-to-government – set the basis for efficient, effective, and logistics-friendly management of security risks across the end-to-end supply chain. A further implication is that SCS research could use game theory, institutional theory, and supply chain integration as the basis for developing mutually satisfying solutions for securing the supply chain. Let us briefly consider effects of four modes of coordination - logistics synchronization, information sharing, incentive alignment, and collective learning – as suggested by Simatupang et al. (2002). The logistics synchronization aims us to locate and time security controls into the logistics network in a way that meet targeted security level with the least effect on quality, cost, and speed of business logistics. The information sharing among supply chain stakeholders increase ability to design effective risk-based preventive security measures and to detect and respond to criminal activities and to investigate crime. The alignment of incentives across the supply chain partners helps overcome resistance for supply chain security implementation. The fourth mode of coordination, the collective learning, supports sharing of best practices and strategic intelligence within and across organizational boundaries.

The distinction between sources and consequences of supply chain crime risks enables us to observe three different meanings of the term supply chain security. In one sense, supply chain security refers to the degree to which security solutions are capable of protecting the supply chain from criminal activities. In another sense, supply chain security is a state of being secure, intact by criminal exploitation. In the third sense, supply chain security refers to the SCS solutions, or means for mitigating the risk of criminal activities. To sum up, supply chain security can refer to (i) a capability to protect, (ii) a state of being intact, or (iii) means for pursuing security.

Further, the notion of *security* risk emphasizes the possible consequence of criminal activity – breach in the secure state of the supply chain. By contrast, the notion of *crime* risk draws attention to the risk sources - the underlying criminal activities. It is important to note that security risks and crime risks refer to the same type of risks, the latter term just emphasizes the risk source and the previous one the risk consequence. Altogether, supply chain security manages security / crime risks, which arise from criminal activities and pose a risk to the secure state of the supply chain.

4.5. Qualitative case study validation

This section applies the supply chain crime taxonomy to the context Swiss-centric international postal logistics. The purpose of this exercise is to assess the extent to which the taxonomy corresponds the empirical reality. This section settles for discussing only crime problems associated with the postal system; readers seeking for further case study information are guided to study chapters 5 and 6.

Switzerland is generally considered as a tranquil country that benefits from relatively low rates of crime, terrorism, and corruption. All around eight million Swiss residents benefit from high standards of living the country offers in terms of advanced education, healthcare, and infrastructure. Switzerland is politically stable and has a strong economy, famous for banking, pharmaceutical, and watchmaking industries. But although the Swiss postal service is embedded in a fairly safe operating environment, it is exposed to certain crime risks.

Case study interviews reveal that the Swiss postal operator Swiss Post has some problems with crimes that fall into the *theft* class in the supply chain crime taxonomy. To recap briefly, the crimes in the theft class involve unauthorized removal of assets from the supply chain (or in this case the postal system). Swiss Post takes mail theft seriously, as the company considers protection of mail trusted to them as a matter of responsibility, something fundamental they have promised to their clients. Each theft incident means that Swiss Post has failed to do its job: to deliver mail from the sender to the receiver undamaged by promised day. In general, Swiss Post sees that mail theft is a bigger threat to their reputation and the employee safety than to their profits. Recurrent theft incidents would no doubt undermine the Swiss Post's reputation in the eyes of its current and potential clients and lead to loss of business contracts. Overall, the Swiss Post's security and safety manager tells that mail theft is a significant problem that is nevertheless under control: "If you look at the statistics, the percentage of stolen and lost items is very low in relation to the high volume of postal items we process." As a matter of fact, Swiss Post is one of the most reliable postal operators worldwide. In those rare occasions, when postal items get lost somewhere in the postal system, main reasons for the loss are careless handling or inadvertent delivery to a wrong address; theft accounts for a fraction of the lost items[48]. The manager remarks that theft by Swiss Post's own employees tends to be more common than theft by external thieves. In a recent, exceptionally zealous case from early 2014, two sorting center workers were found guilty for stealing valuable contents worth around 100 000 CHF from postal parcels. The reason why the internal employees are more often to blame for theft than the external thieves is that the staff has a legitimate and often unsupervised access to mail. Also,

[48] Swiss Post's theft statistics are confidential, but McCarthy (2009) offers a point of reference: in 2003, Royal Mail attributed 6,6% of total loss of mail in the postal system to theft.

years of experience make some staff members able to recognize those postal items that contain something worth to steal, like credit cards, concert tickets, quality chocolate, or cash. The external thieves often hit at the final delivery stage, especially when postmen leave their delivery vehicles and undelivered postal items unattended. Sometimes mail theft incidents also involve intimidation and violence. The Swiss Post's security manager expresses his concern about post office robberies that occur in Switzerland a few times a year. But more than the frequency or material losses, the problem with the robberies is that they endanger employee safety. Many times robbers carry firearms and resort to intimidation and violence, therefore putting the health of the employees in jeopardy. The robbers, the Swiss Post's manager tells, are often very well organized, and they target mainly cash, not postal items.

Seizure records and anecdotal evidence suggest that the postal system in Switzerland and elsewhere is used to a certain extent to smuggle illegal goods. However, due to its clandestine nature, the extent of trafficking through the postal service is hard to estimate accurately. Available seizure records anyhow suggest that contraband smuggling through the postal (and the courier) service is thriving. The retail value of seized counterfeits, that the customs confiscated from postal traffic at the external borders of the EU, accounted for over 106 million euros in 2012 (EC 2012). Besides the fake products, the postal service is an important channel to smuggle tobacco, illegal narcotics, doping substances, CITES-goods, and dirty money across borders (KLPD 2008; UNODC 2010). Especially the growing illegal e-commerce drives the smuggling through the postal system. Rogue online merchants, similar to law-abiding online vendors, typically sell their products on their websites and ship their merchandise to buyers by post or the express courier service. The rogue online traders also commonly exploit legitimate auction sites like e-Bay, craigslist, and alibaba.com to advertise and sell stolen, substandard, or fake products. Sometimes, the traders set up illegal online pharmacies that vend pharmaceuticals that most often do not meet official quality criteria. The European Alliance for Access to Safe Medicines reports that 62 % of medicines purchased online are counterfeits or substandard, and that over 90% of online pharmacies operate illegally (EAASM 2008)[49]. But most alarmingly, the Internet's dark underbelly, the "deep web", hosts a growing number of anonymous online black markets, which are the most flagrant hallmarks of the dark side of the e-commerce. Vendors at one of the anonymous online trading platforms, Black Market Reloaded, sell anything from fake identities and handguns to doping substances and heroin. The hidden storefront is accessible only through special gateway software, which encrypts Internet traffic before routing it through a network of proxy computers, making it practically impossible to locate the users IP addresses. The digital Bitcoin currency enables sellers and

[49] Very small sample, unclear description of research methods, and funding from pharmaceutical interest groups diminish credibility of these alarming findings.

buyers make deals without traceable money transactions. Before being shut down by the US authorities in 2013, the Silk Road, perhaps the most infamous online black market, moderated transactions worth of around 15 million USD a year (Christin 2012). Alas, despite the unexpected crackdown of the Silk Road, which succeeded because of old-school detective work rather than modern cyber crime investigations, other online black markets continue to prosper.

Swiss Post certainly acknowledges that their service is abused to smuggle illegal goods, and the company wants to avoid the abuse. However, in practice, Swiss Post seems not to be much worried about the smuggling as long as the illegal traffic does not pose a threat to the health and safety their customers and employees, disrupt postal logistics, or ruin the Swiss Post's reputation in the eyes of clients, authorities, or the general public. Otherwise, governmental border control agencies drive the agenda when it comes to preventing and detecting illegal traffic through the postal network. In Switzerland, the postal smuggling is a concern primarily to customs and other border control agencies whose duty is to enforce laws governing international trade and cross-border logistics. The range of contraband the customs target is broad. With respect to the absolute contraband, the customs and border control agencies target mainly narcotics, counterfeits, and less commonly stolen goods and fake IDs. In case of otherwise legal, relative contraband, the customs and border control agencies control for outlaw CITES-goods[50], medicines, doping substances, and cultural artifacts. Fiscal contraband has the lowest priority in the border controls. "It is true that the money raised in the postal and global courier traffic is just a few millions [each year]," a Swiss customs' tax specialist points out. "We raise a few billions [in total] in taxes, so the postal traffic is quite peanuts." Other important trade control agencies include agricultural, health, phytosanitary, and veterinary authorities. The police, that enforce the law inland rather than at the borders, are responsible for fighting the traffic in stolen goods and narcotics. Table 24 concludes the interests of different stakeholders to various types of contraband (absolute, relative, and fiscal) as well as security and safety threats that travel or may travel through the Swiss postal service, either in the domestic or cross-border mail traffic.

Stake-holder	Absolute	Relative	Fiscal	Security	Safety
Cantonal police	"We are in charge of drugs, stolen goods and many others.	No or little interest.	No or little interest.	Homicide squads investigate violent crimes.	No or little interest.

[50] Unauthorized CITES (The Convention on International Trade in Endangered Species of Wild Fauna and Flora) goods comprise endangered live animals and plants as well as a range of products derived from them, including game trophies, bush meat, leather goods, and elixirs of the traditional medicine.

	Those are criminal offences."			
Swiss customs	"For exports, our first priority is the smuggling in strategic goods" (PP) "[For imports,] the secondary priority is drugs, counterfeits, and CITES goods."		"The fiscal threat would be the third priority [regarding imports]."	"In imports, we prioritize explosives, weapons, and radioactive items – I mean the security risks."
Swiss Post	"We transport mail from A to B, and that's it. We do not carry out anti-trafficking controls on behalf of authorities."			"The first priority is the protection of the life and health of our employees, clients, and partners." "Of course we want to avoid dangerous and forbidden mail items onboard planes"
Swiss World Cargo	No or little interest.	No or little interest.	No or little interest.	"Security [and safety] has the highest priority, but it's still only a part of the contract. We also want to make business"

Table 24 Stakeholders' interests in controlling contraband and security and safety threats

Explosive, chemical, and biological threats in the postal network are common concerns for Swiss Post and Swiss government agencies – the customs, the police, and particularly the Swiss Federal Office of Civil Aviation (FOCA). Airmail security is high on the postal security agenda because a single explosive postal item onboard an aircraft could cause massive damages. Luckily, to date, no bombs have found among airmail shipments in Switzerland. On the other hand, far less potent safety threats – mainly sprays, perfumes, and lighters – are taken out of airmail shipments, on a daily basis. Although some safety threats evidently pass the screening process undetected, hazardous articles and substances have not so far caused accidents on flights taking off from Swiss airports. Altogether, including all modes of transport, terrorists have abused the Swiss postal system to move security threats to their target only once. In this sole incident, in March 2011, a group of Italian-based anarchists sent a parcel bomb to the head office of Swissnuclear, a lobby of nuclear energy. The bomb inflicted minor injuries on two office workers who opened the parcel. To date, biological, chemical, or radiological weapons have never been discovered in the Swiss postal system (or even in Europe, to my knowledge). However, Swiss Post encounters "twenty to thirty incidents of unknown [but harmless] substances in sorting centers every year," the Swiss Post's security manager says. Sometimes parcels and envelopes break in the sorting process, revealing the contents. The exposed contents may raise suspicions among sorting staff. "People send sometimes powder sugar or flour just to joke," as the security manager points out. In autumn 2012, a discovery of unidentified white powder triggered in a mass evacuation in the Zurich-Mülligen sorting center and delayed

delivery of 1,5 – 2 million postal items over next few days. All this occurred although the later laboratory testing confirmed that the mysterious substance was harmless starch powder.

At the global level, there have been many infamous mail bomb campaigns (see Table 25). Ted Kaczynski, aka the "Unabomber," terrorized the US society from the late 1970's to the mid 1990's with a series of parcel bombs that killed three people and injured 23 others. In Europe, Franz Fuchs, an Austrian xenophobe, killed four people and wounded several in five mail bomb waves between 1993 and 1995. Later in 2003, an Italian-based far-right extremist group sent seven parcel bombs to prominent EU institutions and politicians in the pre-Christmas "Operation Santa Claus." In 2007, two infamous mail bombers, John Tomkins (aka the Bishop) and Miles Cooper, engaged in their personal campaigns of terror. From the late 2010 to the late 2011, Greek and Italian anarchist groups carried out several mail bomb attacks on political and financial institutions around Europe.

Timespan	Major mail bomb campaign (kills / injuries / bombs)
1978 – 1995	Ted Kaczynski's (aka "Unabomber") terror in the US (3 / 23 / 16)
Dec 1993 – Dec 1995	Franz Fuchs' five mail bombing sprees in Austria (4 / 15 / 28)
Dec 2003 – Jan 2004	The "Operation Santa Claus" parcel bomb attacks on prominent EU figures and institutions (0 / 0 / 7)
Jan 2007	John Tomkins' (aka the "Bishop") mail bombs against US financial institutions (0 / 0 / 2)
Jan – Feb 2007	The Miles Cooper's mail bomb campaign in the UK (0 / 8 / 7)
Nov 2010	Greek anarchists' mail bomb campaign against embassies and high level politicians (0 / 1 / 10)

Table 25 Major past mail bomb campaigns

Terrorists have exploited the postal service to also distribute noxious chemical or biological agents in so-called white powder letters (see Table 26). The most infamous incidents date back to late 2001, when four letters enclosing Anthrax spores killed five and infected 17 victims only a few weeks following the September 11th attacks. Between October 2003 and February 2004, a terrorist dubbed as "Fallen Angel" mailed three ricin-tainted letters to major US political institutions. Next time ricin letters were discovered in the US system in 2013, when apparently unconnected ricin-laden letters were sent to President Obama, a few other high profile US politicians, and a judge. Besides the actual attacks, there have been many hoax attacks involving seemingly dangerous substances and/or threatening messages. It should be noted, however, that anthrax, ricin, or other toxic weapons have never been found outside the US mail system,

or at least media has not reported about such incidents. However, the risk of distribution of weaponized pathogens and chemicals through the postal service is a serious threat that can lead to major losses. This is why the US postal service, for example, still uses significant amounts of money and resources to prepare for the risk of bioterrorism in the postal system.

Timespan	White powder letter campaigns (kills / injuries / letters)
Sep – Oct 2001	The "Amerithrax" anthrax letters (5 / 17 / 4)
Oct 2003 – Feb 2004	The three "Fallen Angel" ricin letters in the US (0 / 0 / 3)
Apr 2013	Ricin letters to President Obama, a senator and a judge (0 / 0 / 3)
May 2013	Shannon Richardson's ricin letters to President Obama and New York city mayor (0 / 0 / 2)

Table 26 White powder letter attacks

Some crime problems in the postal logistics network fall into the *direct attack* class. Owing to the dense countrywide postal infrastructure, it is common that post office windows get stoned, public mailboxes battered, or delivery vehicles sprayed somewhere in Switzerland. Such situational vandalism is mainly conducted by external people. It is also possible that disgruntled former or current employees sabotage the postal infrastructure operations to get their revenge. Besides material damages, aggressive customers sometimes cause disorder in post offices and intimidate clients and staff. The Swiss Post's security manager assumes that such offences are typically impulsive. The post office robberies could be included into the *direct attack* class as well because the robberies, as described earlier, involve direct attack on supply chain infrastructure and personnel.

The case study evidence suggests that many postal crimes involve elements of facilitating crime. The Swiss Post's security manager noted that insider information sometimes facilitates theft of postal items. "Some employees have revealed detailed security measures to external people," the manager tells. "So insider knowledge is used both by insiders themselves and external people." The insider information allows postal staff members to recognize the most attractive items to steal, to circumvent anti-theft controls, and to make theft investigations more difficult for the Swiss Post's internal investigators and the police. As an illustrative example outside Switzerland, a former postal employee managed to break into a sorting center and steal around 200 registered and priority letters in Finland. Professional robbers also evidently abuse the insider information to plan their attacks on post offices. The insider information also plays a critical role in smuggling through the postal system. For example, on a forum of one the anonymous online blackmarkets, a former UPS employee provides a detailed walkthrough of the US export procedure and shares tips for avoiding customs controls. This anecdote illustrates

that not all employees that express couriers or postal operators hire maintain their integrity during and after their employment. The insider information may cause the biggest problems in the airmail channel. The trustworthiness of people working with identifiable airmail is generally high because of background vetting and training they undergo before hiring and because of the relatively low staff turnover in airmail handling facilities. However, it is possible that hostile actors succeed to infiltrate into the airmail facilities. As a sad reminder, one airmail handler killed two and wounded several US soldiers in Germany in March 2011. The German police attributed the radicalization of the offender, who did not have a criminal background, to online Jihad propaganda[51].

Aside the abuse of the insider information, other common facilitators of the postal crime include the use of fraudulent documents and the use of violence and intimidation. Smugglers of CITES-goods, medicines, and cultural artifacts often forge licenses, certificates, and other trade documents to deceive border control officials. The use of violence and intimidation is typically involved in the post office robberies and sometimes in the sabotage and the vandalism. Otherwise, despite the relatively rich case study evidence I collected, no links were found between the postal crime and corruption, cyber crime, or identity theft. The absence of evidence, however, does not imply the absence of possible linkages. It is rather safe to assume that somewhere in the world, if not in Switzerland, these facilitating techniques are employed to commit postal crime. Table 27 below summarizes how the identified crime problems in the Swiss postal logistics system map onto the taxonomic classes.

	Taxonomic class	Crime concerns in the Swiss logistics network
1	Theft	Frequent cases of internal pilferage and theft by external thieves. Occasional violent post office robberies, often committed by professional criminal groups.
2	Smuggling	Authorities and Swiss Post are aware that the postal service might be abused in smuggling.
	Absolute	Narcotics, counterfeits, money
	Relative	Medicines, doping substances, CITES goods
	Fiscal	Fiscal contraband (e.g., undeclared cigarettes) is a minor problem because Swiss customs collect only a little portion of taxes and duties from the postal traffic.
	Contractual	Not reported.
	Safety	Swiss Post removes dozens of hazardous articles and substances – mainly sprays, perfumes,

[51] Switzerland's security. Situation report 2012 of the Federal Intelligence Service FIS.

		and lighters – from airmail shipments each day.
	Security	One mail bomb incident in the last twenty years. No biological, chemical, nuclear, or radiological attacks.
3	Direct attacks	Daily cases of vandalism. Occasional assaults on employees and property.
F	Crime facilitation	Abuse of insider information, violence, and intimidation were mentioned.

Table 27 Taxonomic classes and Swiss Post's crime threats

For the most part, the taxonomy covers all crime problems that emerged from the case study data. However, there were some overlaps between taxonomic classes and crime types. It was not clear whether the post office robberies correspond more accurately the *theft* class or the *direct attack* class. After all, on the other hand, the robberies involve removing assets (mainly cash) out of the postal system, and thus the crime type fulfills the requirement of being categorized as a type of theft. However, the robberies often are violent events. In this sense, the robbery also fulfills the inclusion criterion of the *direct attack* class. But despite this single overlap between the two taxonomic crime classes, the taxonomy seems to correspond quite accurately the reality (or its case study approximation). Another issue with the validity is that the case study data lacks evidence of certain supposedly important facilitating crime types. In particular, no evidence was found that cyber crime or corruption would be anyhow relevant facilitators of the postal crime. Even so, despite these minor inconsistencies, it seems that the taxonomy reflects the crime risk environment in which the Swiss postal logistics network is embedded. However, future research should put these initial, encouraging findings into further test.

Summary

This chapter characterized supply chain security risks and created a taxonomy of supply chain crime types by analyzing managerial descriptions of crime problems that occur or could occur in the supply chain context. The analysis revealed that supply chain crime problems are numerous and diverse, most important being cargo theft, smuggling, and cyber crime. This diversity of the crime problems collapses into three main taxonomic crime classes when categorizing the problems based on the way how criminals interact with the supply chain: 1) by taking assets out of the supply chain, 2) by introducing contraband into the supply chain, and 3) by attacking supply chains directly. Besides the main ways of interaction, criminals and terrorists commonly employ a range of facilitating techniques to support their main criminal activities. The characterization of security risks allowed us to differentiate supply chain security

from supply chain risk management, its apparent parental discipline. Further, the research allowed us to clarify key supply chain security terminology and identify tools and theories that most likely help mitigate security risks in the supply chain context. The chapter concluded by highlighting some additional differences across the three main taxonomic classes and by assessing the validity of the taxonomy by applying it to the context of the Swiss-centric international postal logistics.

Chapter 5 | Case study description

This case study chapter depicts the international postal service from the Swiss perspective, putting a special emphasis on supply chain security and law enforcement. The chapter starts with an introduction to Swiss Post and its core postal operations before proceeding into details of postal security management in the Swiss-centric cross-border postal logistics network. The last section wraps up the case study description by mapping the identified postal security domains onto the baseline postal logistics process.

5.1. Overview of the international postal service

The first section of the case study takes a look on basic international postal services and major trends that are reshaping the global postal business. The section clarifies key differences between the cross-border postal, the express courier, and the freight logistics services and details a range of goods and commodities that, if certain conditions are met, can be sent through the international postal service.

5.1.1. Basic postal services

The Universal Postal Union (UPU) coordinates postal policies and operations across its 192 member countries. The members have agreed to comply with the UPU's convention and its regulations that set common rules for the international postal service worldwide. The combined network of the 192 UPU Posts, "the single postal territory," covers virtually the whole world. The global postal logistics system handles around 350 billion letters and 6 billion parcels a year, of which 3,7 billion letters (1,1 %) and 57 million parcels (1,0%) are delivered internationally (UPU 2012). The international postal traffic brings around 4% of revenues for the postal operators. The global postal logistics has a huge scale, but it also has a significant economic impact. In 2012, the postal operators employed 5,5 million people worldwide (UPU 2012). In the European Union, the postal services accounted for nearly 0,6% of the gross domestic product.

Among other provisions, every member country must designate a postal operator (referred Posts throughout this thesis) that is responsible for providing "quality basic postal services at

all points in their territory, at affordable prices" (UPU Convention Art. 3). The basic postal services cover acceptance, handling, conveyance and delivery of priority and non-priority letter-size items (letters, cards, and small parcels up to 2kg) and parcels (up to 20kg). However, many countries oblige their postal operators to provide additional services beyond the basic postal services, as defined by UPU. These so-called universal service obligations (USO) vary from country to country, but typical USO regulations determine product range, covered area, service frequency, price, and quality criteria for the national postal system (Jaag 2007).

To offset the burden of the Universal Service Obligation (USO), some governments allow their national postal operators hold legal monopolies. In Switzerland, for example, Swiss Post holds a legal monopoly for letters up to 50 grams. Today, many countries have opened or are opening their postal markets for competition. In the European Union, the directive 2008/6/EC ordered the full opening of the postal markets in sixteen member states from the beginning of 2011. As a result, around 95 percent of the EU's internal postal markets are currently liberalized, meaning that also companies, which are free of universal service obligations, may provide postal services. The market liberalization advances in parallel with so-called corporatization of the postal operators. Many governments are reducing their control and ownership in their national Posts with intent of transforming "rigid" postal administrations into entrepreneurial market-oriented modern businesses. The Dutch postal operator, Post NL, is currently fully privatized whereas the German Deutsche Post DHL and the Austrian Österreichische Post are examples of mixed state-private ownerships. In Switzerland, the government has converted the Swiss Post's business structure from the public institution into the public limited company while retaining full ownership.

5.1.2. Differences between postal, express, and freight logistics

The Universal Service Obligation and the remnants of legal monopolies are not the only characteristics that differ the postal service from freight and express courier service (see Table 28). Posts generally accept shipments weighting up to 30 kg while most courier companies carry goods and documents up to 70 kg per shipment. Freight transport takes care of heavy, bulky, and hazardous shipments which transport is beyond the capabilities of the postal and express courier systems. In particular, freight companies commonly handle unitized cargo (e.g., pallets and containers), voluminous bulk deliveries (e.g., crude oil and grain) or project cargo (e.g., wind turbines and missiles). Postal and express couriers transport goods between a large number of senders and recipients while the freight companies typically have a more consolidated customer base that comprises mainly business clients, which ship in large volumes and quantities. The four dominant express courier giants, UPS, FedEx, DHL, and TNT, control their entire international door-to-door logistics network owing to their global presence and own fleet of airplanes. The Posts in turn have an unrivalled local presence owing to their

countrywide post office networks and numerous delivery staff. But despite the strong national presence, unlike the express couriers, Posts must always collaborate with others postal operators when it comes to the international logistics. The integrated door-to-door service of express couriers outperforms the postal service in terms of speed and time-certainty. Yet, superior service comes at high cost. It is well said that the express courier service is the "business class for cargo" (Oxford Economics 2011). The fastest time-definite delivery options are not available for the postal or freight shipments. Unlike postal and express courier services, general freight relies strongly on considerably slow but cheap maritime shipping.

	Market		
Characteristics	Postal	Express	Freight
Universal Service Obligation	Only for Posts	No	No
Legal monopoly	Sometimes for Posts	No	No
Average weight & size of shipment			
Share of business clients			
Number of senders & recipients			
Speed, price-per-kilo, and time-certainty of delivery			

Table 28 Characteristics of postal, express and freight services

5.1.3. Range of mailable items

The postal logistics infrastructure sets technical constraints for the postal items in terms of contents, packaging, weight and dimensions. The maximum weight for any postal shipment is between 20 – 30kg, depending on country of origin and destination. The character of the postal logistics also restricts transport in bulky, perishable, and fragile goods as well as commodities that require transportation in certain temperature, humidity, or under other special conditions.

A broad variety of commonly traded goods have explosive, flammable, oxidizing, infectious, radioactive, corrosive or ecologically hazardous properties. Dangerous goods regulations classify such hazardous commodities and set provisions for their handling, packaging, labeling, marking, and segregation across various modes of transport (see Table 29). Most governments have integrated so-called UN recommendations on the transport of dangerous goods into

national legislations. The UPU's letter and parcel post regulations[52] prohibit the mailing of these dangerous goods by post, at least for the most part. Some Posts carry certain dangerous goods – sprays and aerosols and other consumer products containing small amounts of dangerous substances – in limited quantities. However, Posts accept dangerous goods mainly for the surface carriage and on a contractual basis. Only three types of dangerous goods are allowed for the air carriage under safety provisions: patient specimens, certain infectious substances, and low-activity radioactive materials.

Instrument (abbreviation)	Legal basis	Scope (contract parties)
The European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR)	Standalone binding agreement	Mainly Europe (47)
Regulations concerning the International Carriage of Dangerous Goods by Rail (RID)	Appendix C of the COTIF convention	Mainly Europe (47)
ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air (ICAO-TI)[53]	Annex 18 of the Chicago Convention	Global (191)
The International Maritime Dangerous Goods Code (IMDG Code)	SOLAS convention	Global (162)
European Agreement of Dangerous Goods by Inland Waterways (ADN)	Standalone	Europe (17)

Table 29 Conventions regulating transport of dangerous goods

The process technical restrictions, UPU universal principles[54], and company policies set limitations to the postal traffic. National legislations set the legal basis for possession, transport, handling, import, transit, and exports of goods, and consequently the de jure range of mailable items. As the legal restrictions vary across countries, the range of mailable items depends on the laws and statuses in the country of origin, the country of destination, and possible transit countries. Figure 9 below summarizes the rules that determine the range of mailable items.

[52] Art. RL 144 and Art. RC 133

[53] The IATA's Dangerous Goods Regulation is the de facto practical guidance for the aviation industry although it is not legally binding.

[5454] The UPU Convention defines what kind of items, and under which conditions, Posts can accept for international delivery. Among other articles, the Convention prohibits postal traffic in illegal drugs, obscene and immoral material, counterfeits, most live animals, and dangerous goods.

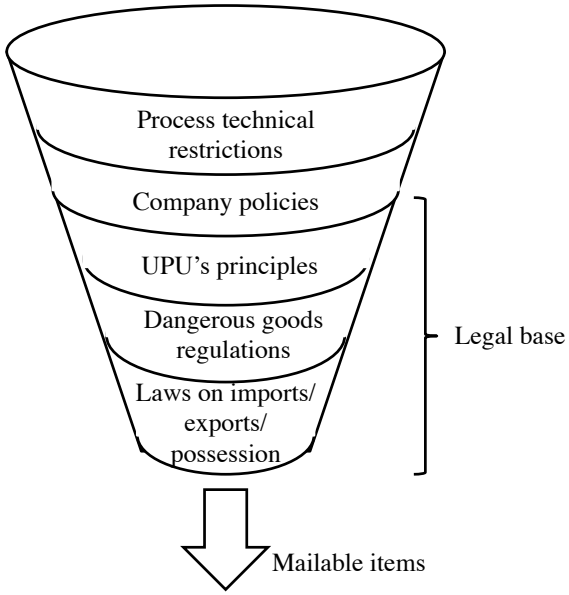


Figure 9 Determinants of mailability

5.2. International postal logistics in Switzerland

This section frames the context where the Swiss postal service takes place. The following pages introduce Swiss Post group and its business units that are responsible for running the postal service and fulfilling the universal service obligations (USO), as laid down in the Swiss postal law. The text portrays the postal logistics infrastructure in Switzerland and key postal logistics processes involved in the cross-border exchange of postal items.

5.2.1. Swiss postal service

Switzerland, the focal country of this case study, has its distinct characteristics that affect how the postal service is arranged. Like other UPU member countries, Switzerland has assigned a designated operator (Swiss Post), a regulatory authority (PostCom, former PostReg), and a governmental authority (DETEC[55]) to take care of the provision of basic postal services in its territory. Being the "designated operator" in Switzerland, Swiss Post must comply the Universal Service Obligations (USO) as defined by the Swiss postal law (RS 783.0). Among other stipulations, the postal law obliges Swiss Post to transport letters (items less than 2cm thick, up to 2kg), parcels (items more than 2cm thick, up to 30kg), newspapers, and periodicals at least five days a week to all permanent settlements throughout the 41285km^2 large Swiss territory, which covers densely populated Swiss plateau and less populous, mountainous areas in the south and southeast parts of the country. The universal service obligation also stipulates

[55] The Federal Department of the Environment, Transport, Energy and Communications

uniform pricing for domestic mailings of the same type and class: posting a domestic A-Mail standard letter costs always 1.00 CHF regardless of the distance between the sender and the addressee. The postal law also states that people living in Switzerland, whether living in cities or remote Alpine villages, should also have a "reasonably" convenient access to the postal services. To compensate inconvenience of complying with the USO, the Swiss law grants Swiss Post a legal monopoly to deliver letters up to 50 grams in Switzerland.

5.2.2. Swiss Post Group

Swiss Post is a multi-sector public limited company that is fully owned by the Swiss Confederation. The federal act on organization of Swiss Post (RS 783.1) sets the legal base for company's operations, structure, and financing. Swiss Post deserves its nickname "yellow giant" as it employs around 44 600 people (full-time equivalents), being the second biggest employer in Switzerland after the retail chain Migros. In 2011, the Swiss Post group generated turnover of 8 582 million CHF and profit of million 859 million CHF. Overall, the Swiss Post group encompasses three strategic subsidiaries: Post Auto AG operates public passenger transport in Switzerland and abroad; Post Finance AG provides retail banking services; and Post CH AG offers a range of logistics and communication services. Post CH AG, or more precisely its four business units, run the Swiss postal service and fulfill the related universal service obligations. The Post Mail unit handles letter-size items (< 2cm thick, < 2kg) while the Post Logistics unit takes care of parcels and freight beyond the letter-size. Post Offices & Sales control the nationwide post office network. The fourth unit, Swiss Post Solutions, offers integrated special services that build on the Swiss Post's brand and the postal logistics system. Figure 10 summarizes Swiss Post's recently reformed group structure and displays revenues and number of staff by business unit.

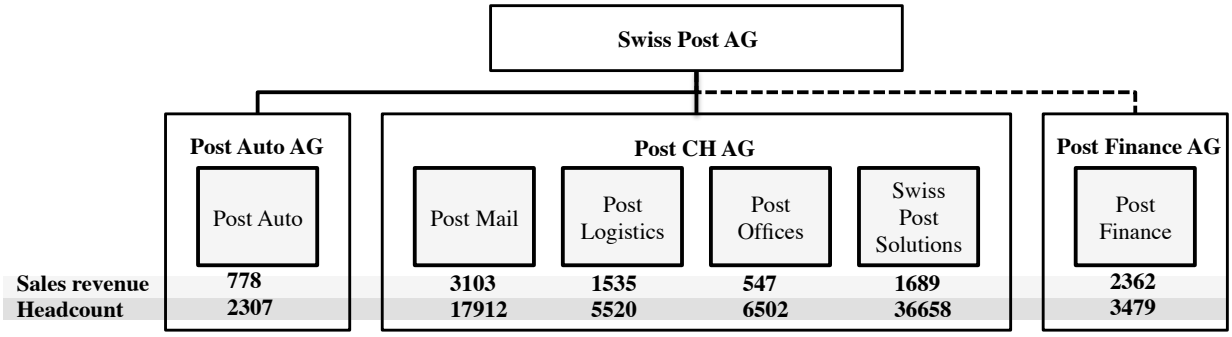


Figure 10 Swiss Post group structure

Over the past years, Swiss Post has become a full-fledged logistics and information service provider through international expansion and diversification into new business areas. In the open logistics market, outside the legal monopoly for less than 50 grams heavy letters, Swiss

Post's logistics and mail units compete mainly with the Swiss branches of the global express couriers FedEx, DHL and UPS. Figure 11 illustrates the differences between logistics markets and highlights the Swiss Post's current market position.

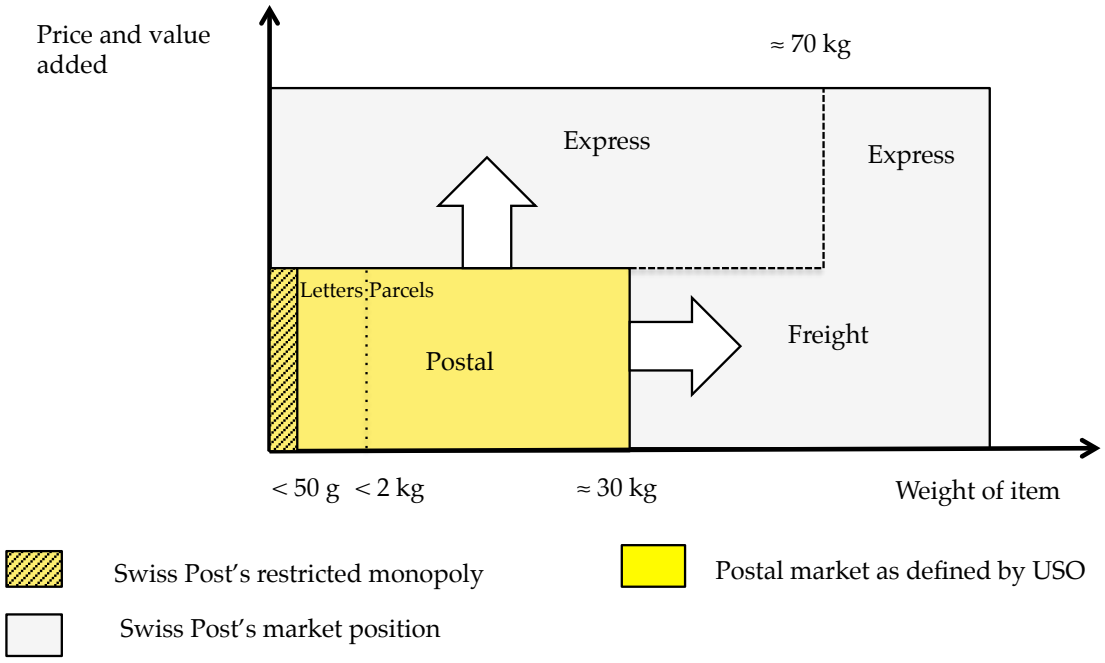


Figure 11 Swiss Post's diversification to new logistics markets

Like most Posts elsewhere in first world countries, Swiss Post is confronted with the challenge of redefining the their role in changing business environment that is characterized by intensifying competition, declining letter-post volumes, and expanding e-commerce markets. The Swiss Post's recent business development projects are largely driven by major trends that are reshaping the postal business worldwide. Advancements in information and communication technologies are shifting demand from letters to small packets and parcels. Over 2006 – 2011, Europe and CIS[56] countries experienced 5,4 % average annual growth rate in international parcel volumes (UPU 2012)[57]. Diege et al. 2013 estimate that in most industrialized countries[58], the volume of cross-border small packets will continue to increase by 4% per year over 2013 and 2017. Meanwhile, the growth of the domestic parcel traffic is projected to level out. Over the same four-year period, Diege et al. (2013) assume, the volume of cross-border letters (small envelopes) will decline by 4% per year and the volume of cross-border flats (large

[56] CIS (Commonwealth of Independent States) countries comprise of former Soviet republics Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, and Uzbekistan.

[57] Average annual growth rate = $\sqrt[5]{}$(parcel volume in 2011 – parcel volume in 2006) = $\sqrt[5]{}$(53,1-40,9) ≈ 5,4%

[58] The analysis considers 24 most industrial countries: AT, BE, DE, DK, FI, FR, El, ES, IE, IT, LU, NL, PT, SE, UK, NO, IS, AU, CA, IL, JP, NZ, CH, and US.

envelopes) will decline by 5% per year. Figure 12 below summarizes major trends that are reshaping the postal industry.

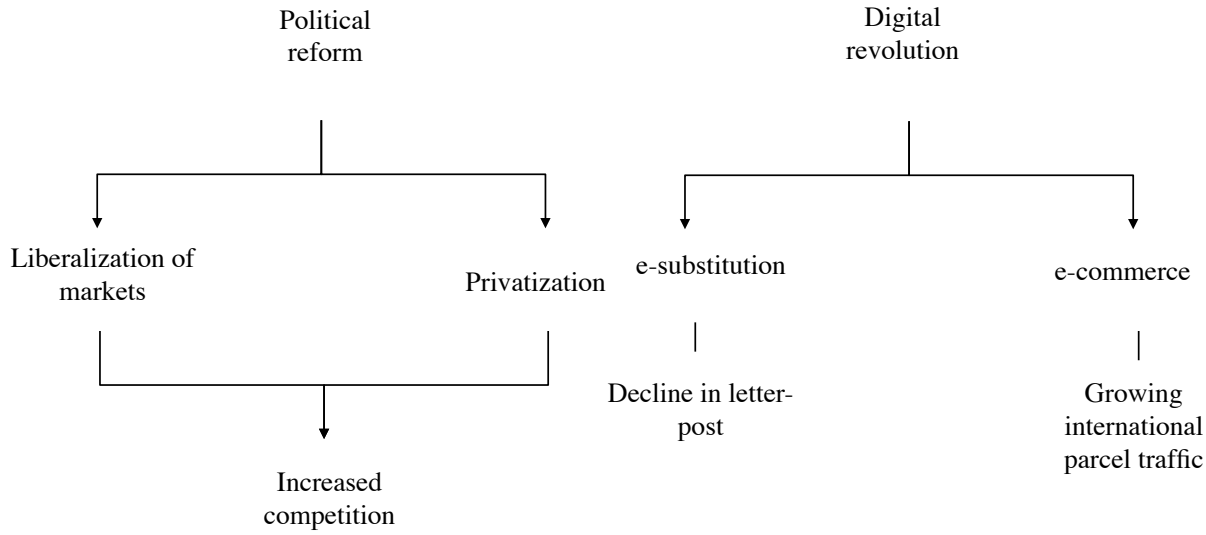


Figure 12 Major trends in the postal business

The Swiss postal network encompasses around 15000 public mailboxes, 1850 post offices, 430 partner outlets, and numerous logistics bases and distribution branches (see Figure 13). Swiss Post operates six sorting centers – three for parcels and three for letter-size items. All international surface traffic goes through Zürich-Mülligen exchange office. Airmail is handled either at Geneva or Zurich[59] airports in airmail exchange offices. Around 16500 mailmen take care of mail delivery to private mailboxes and of collection from public mailboxes. On average, a mailman covers an area of 4,1 km^2 and around 350 households on average, when considering that there are around 3,5 million households across the 41000 km^2 Swiss territory. To support the mail delivery and collection, Swiss Post operates a fleet of around 12500 trucks, vans, mopeds, and other motorized delivery vehicles. Swiss Post also moves mail also by rail when possible and by air when necessary.

[59] The Geneva airmail exchange office deals mostly with imported airmail consignments and all types of express shipments. Most airmail shipments, which depart from Geneva, stop in Zurich where they are transferred to a foreign-bound plane.

Figure 13 Swiss Post's post office network

Swiss Post handles around 2600 million letter-size items and 111 million parcels a year. This makes, on average, 50 million letters and 2 million parcels over the six weekly working days when mail is delivered. This huge volume of letters, parcels, and other postal items is sent by several million private mailers and around 130000 business clients. Switzerland has one of the world's highest mail pieces / capita ratios: each Swiss resident, receives 313 letter-size items a year on average. The international traffic accounts for around 10% of the total traffic Swiss Post handles. In year 2012, Swiss Post handled 274,1 million international postal items, of which 268,6 million were letter-size items and the remaining 5,5 million parcel-size items. Postal exports accounted for 33% of the international traffic and the imports for 67%. Based on the UPU's principles of "the freedom of transit" and "the single postal territory," Swiss Post exchanged postal items with every other UPU member either directly or indirectly through intermediary Posts in one or more transit countries.

5.2.3. Logistics phases

This section illustrates the main phases in the internatinal end-to-end postal logistics process: collection, sorting, export, transit, air carriage, import, and delivery. It is important to note that each logistics phase is descibed from the Swiss perspective. This Swiss-centric presentation is somewhat counterintuitive because international postal items are always processed in two or more countries (the country of origin, the country of destination and possibly one or more transit countries). Swiss-origin international items, therefore, undergo collection, sorting, export, and possible air carriage procedures in Switzerland, as described in the pages to follow. But once abroad, beoynd the Swiss borders, the exported items might experience transit, import, sorting, and delivery procedures that differ substantially from the processes I describe

here. Likewise, the described import, sorting, and delivery phases apply to the Swiss-bound international postal traffic only. But again, in foreign countries, before entering Switzerland, the imported items might have been subject to special handling that differs from the Swiss procedures. Moreover, I discuss here mainly basic logistics phases and only briefly describe associated security and customs procedures. The following sections are dedicated to more detailed elaboration of security and customs activities.

The first logistics phase the postal delivery process is the collection of mail items. Many postal items enter the postal system through public public mailboxes and post offices. Partner agencies, typically located in rural areas and run by local shopkeepers, complement the network of the post offices and thus improve citizens' accessibility to the postal services. Business clients may leave their daily their mailings at non-attended mail drop locations (called SME-points) or request Swiss Post to pick-up mailings. Big business mailers often bring their items, especially material for large mailing campaigns, directly into postal logistics bases or sorting centers. Private customers most often drop their postcards, letters and small parcels into public mailboxes. If a customers wants to send large or special items (e.g., registered letter), a visit to a post office or a partner agency is required. The pick-up service is currently available for private customers if they return mail ordered goods (pick@home), they live in rural areas (home service), or if they pay extra for the express service. Quite recently, Swiss Post has also introduced fully automated parcel drop stations.

After the customers have sent their mailings through one of the access points to the postal system, postal vans and trucks transport the postal items into sorting centers. In this sorting phase, letter-size items are brought to one of the three regional mail sorting centers where they get segregated by class, weight, and format (= dimensions). International mail, in particular, gets sorted into small letters (P, < 100g), large flat letters (G, < 500g), and bulky letter packets (E, < 2000g), according to UPU standards. After aligning, orientation, and other preparatory handling tasks, the mail pieces are routed to right destination and sometimes sequenced for mailmen's' delivery routes. Before leaving the sorting center, workers typically consolidate multiple mail pieces into pouches, bundles, trays, or other mail aggregates, called "receptacles". Depending on the final destinations, the items continue to the international, national, or the regional distribution, or directly to the local delivery. Meanwhile in the parcel channel, the items beyond the letter-size (> 2kg or > 2cm thick) are brought in one of the three parcel sorting centers. After workers have unloaded incoming parcels onto the conveyance belt of the oval-shaped sorting system, various sensors register weight, dimensions, address information, and barcode identifiers of each parcel in motion. Based on the address information, the sorting system routes the parcels to the right loading bay for a connection transport. Figure 14 below illustrates some key sections in the parcel sorting process.

a) b) c)

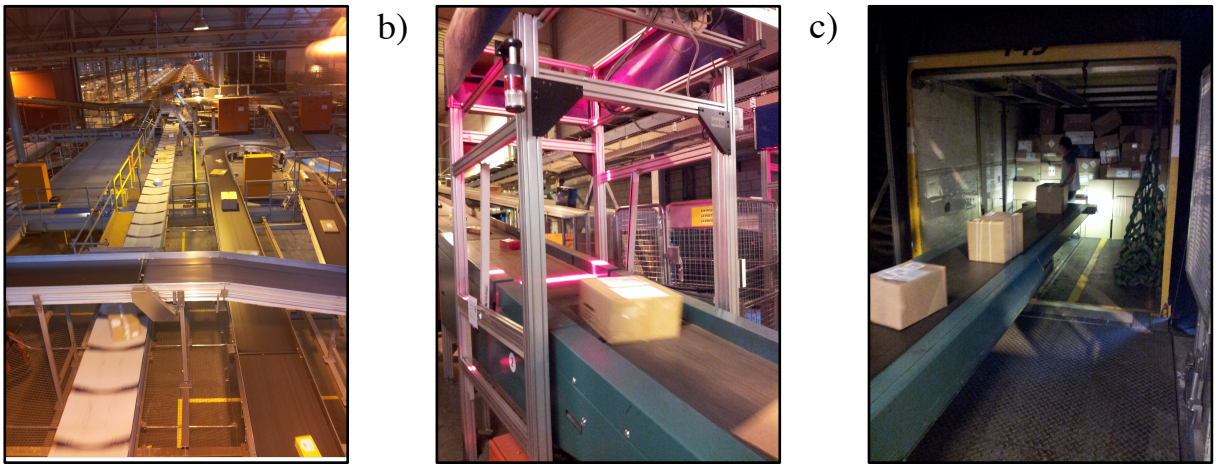


Figure 14 Parcel sorting center: a) conveyance belts b) infrared bar-code reader c) loading bays

Foreign-bound items proceed to export logistics phase before exiting the Swiss territory. In this phase, Swiss Post's customs brokers prepare the export declarations for items if the contents are worth more than 1000 CHF, the contents are subject to export restrictions, the shipment requires a certificate of origin, or if the shipment encloses watches, jewelry, or other valuables. Otherwise the brokers declare letters and parcels in multi-item batches by providing customs only consignment-level exit notifications, containing information on country of destination, class and aggregate weight of the items, and estimated time of departure. Being an authorized consignor (expéditeur agrée), a trusted trader in the Swiss customs' view, Swiss Post may use simplified export declarations, declare outbound postal items from their own premises, and benefit from flexible opening hours of customs offices.

The next air carriage phase concerns only a part of the export traffic. For the most part, Swiss Post exchanges letters and parcels with its neighbors France, Germany, Austria, and Italy by road and with other countries by air. Accordingly, this means that nearly 55% of international mail volumes enter and exit Switzerland by air. However, despite the dominance of the air carriage in the international postal service, around 2% of the total volume Swiss-origin mail, including both the domestic and international traffic, travels by air.[60] In 2008, the Swiss Post's "strategic carrier," SWISS World Cargo, flew around 17 000 tons of mail, meaning that each SWISS flights carried nearly 130 kg of mail on average[61] [62]. At the global level, airmail accounts

[60] Assuming that the cross-border postal traffic mirrors the Swiss foreign trade flows [Exports / (Exports + domestic traffic)] × % of exports taking plane = [90 / (90 + 2310)] × 55% = 2,1%

[61] Computed based on figures presented in Business magazine SwissWORLD Cargo "Cargo Matters" Issue 2, 2009 and the annual report of its parent company SWISS in 2009.

[62] Although the exact airmail volumes are unavailable due to confidentiality reasons, a representative of SWISS World Cargo assures that carrying mail is very common. "If we hadn't mail, it would be a big hole in the revenue in the overall cargo and mail business."

for over 65% of the international mail volume (IPC 2008) and 3,4% of the total global airfreight measured by revenue-tonne kilometers (Boeing 2012), being a billion dollar business for airlines.

Swiss Post uses the air carriage depending on the distance and urgency of postal items. Therefore, rather surprisingly, both priority and economy class items may be carried by air. Instead of talking about economy and priority class mail, airlines generally recognize three air-mode-specific types of mail, which determine handling and space allotment priority: express mail (EMS), priority mail, and surface air lifted (SAL) mail (i.e., the economy items). The priority and SAL categories consist of letters and parcels up to 30 kilos, which travel under the rules of the Universal Postal Union. Swiss Post tenders airmail consignments to air carries after a third party security service provider has screened airmail items for security and safety threats. Figure 15 presents some pictures from the airmail handling process.

a)

b)

c)

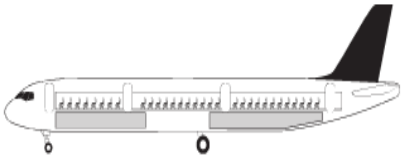


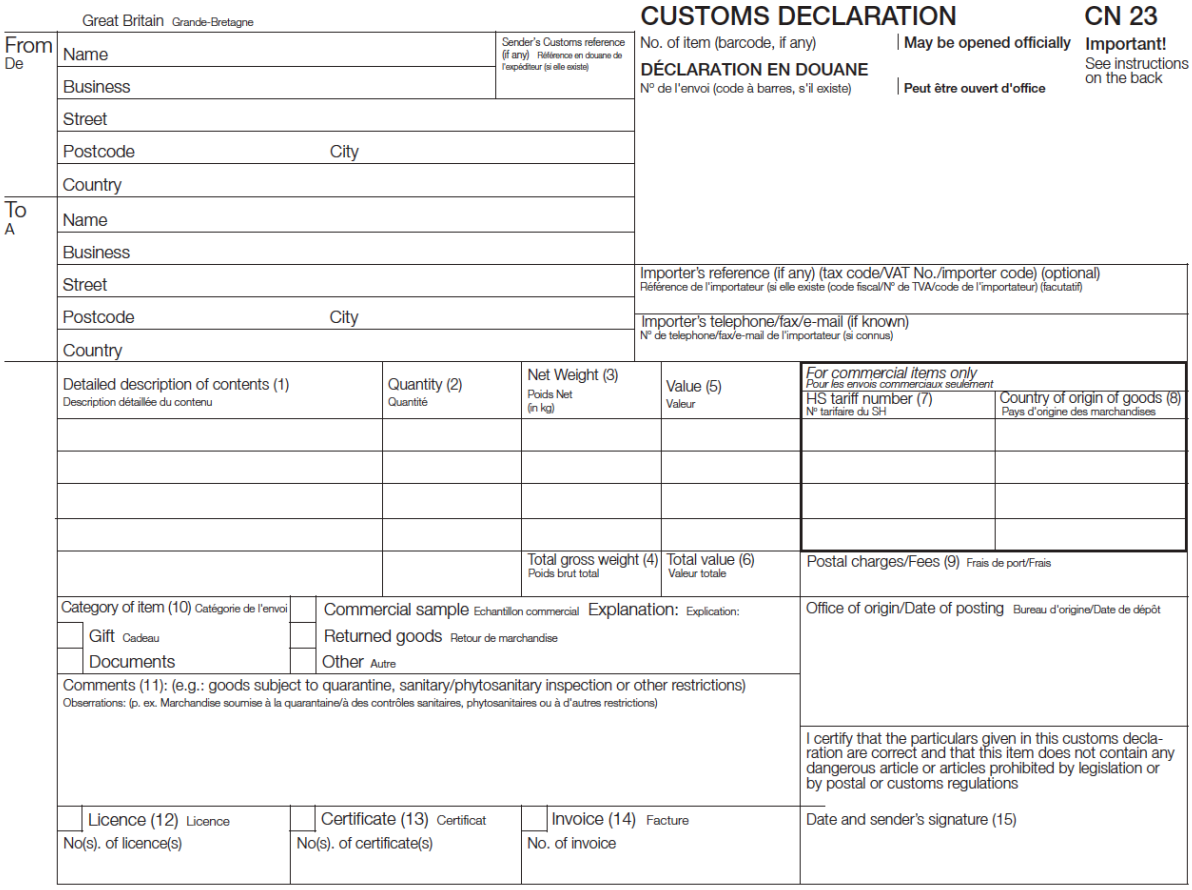
Figure 15 Airmail process pictures: a) Air cargo container (= unit loading device or ULD), b) mailbags, c) under cabin cargo compartment(s) [63]

Owing to the authorized consignee status (destinataire agréé)[64], Swiss Post can transport surface mail directly to the Zurich-Mülligen exchange office, located at the outskirt of Zurich, without being stopped and inspected at the border or customs offices. Airmail arrives directly into airmail exchange offices in Zurich and Geneva. When the postal items arrive in one of the exchange offices, they go through an import clearance process in which Swiss Post's customs brokers prepare official, legally binding import declaration for each item. The brokers use information of standard UPU customs declaration forms CN22 and CN23 (see Figure 16) that

[63] Source: Jettainer brochure, www.cds-worldwide.com, wikipedia article (ULD)

[64] The Swiss customs grant the authorized operator licencse DA to companies that export sufficient amount of goods in a year, employ competent customs brokers, financially solvent, and have an excellent track record of customs compliance over the last three years (Procedures simplifiées pp. 3). Main benefits of the DA status are declaration from own premises, flexible hours of customs offices, and possibility to use simplified import declaration.

accompany most parcels and envelopes. Sometimes the brokers open the items and verify the contents or take a look on regular or pro-forma[65] invoices so that they can compute duties and taxes accurately. The brokers produce the items to customs for examination should the customs request them to do so.


Great Britain Grande-Bretagne

CUSTOMS DECLARATION **CN 23**

Important! See instructions on the back

From / De — Name; Business; Street; Postcode City; Country

Sender's Customs reference (if any) Référence en douane de l'expéditeur (si elle existe)

No. of item (barcode, if any) **DÉCLARATION EN DOUANE** N° de l'envoi (code à barres, s'il existe)

May be opened officially **Peut être ouvert d'office**

To / A — Name; Business; Street; Postcode City; Country

Importer's reference (if any) (tax code/VAT No./importer code) (optional) Référence de l'importateur (si elle existe (code fiscal/N° de TVA/code de l'importateur) (facutatif)

Importer's telephone/fax/e-mail (if known) N° de telephone/fax/e-mail de l'importateur (si connus)

Detailed description of contents (1) Description détaillée du contenu	Quantity (2) Quantité	Net Weight (3) Poids Net (in kg)	Value (5) Valeur	*For commercial items only* Pour les envois commerciaux seulement: HS tariff number (7) N° tarifaire du SH	Country of origin of goods (8) Pays d'origine des marchandises
		Total gross weight (4) Poids brut total	Total value (6) Valeur totale	Postal charges/Fees (9) Frais de port/Frais	

Category of item (10) Catégorie de l'envoi: ☐ Gift Cadeau ☐ Documents ☐ Commercial sample Echantillon commercial ☐ Returned goods Retour de marchandise ☐ Other Autre — Explanation: Explication:

Comments (11): (e.g.: goods subject to quarantine, sanitary/phytosanitary inspection or other restrictions) Observations: (p. ex. Marchandise soumise à la quarantaine/à des contrôles sanitaires, phytosanitaires ou à d'autres restrictions)

Office of origin/Date of posting Bureau d'origine/Date de dépôt

I certify that the particulars given in this customs declaration are correct and that this item does not contain any dangerous article or articles prohibited by legislation or by postal or customs regulations

☐ Licence (12) Licence	☐ Certificate (13) Certificat	☐ Invoice (14) Facture	Date and sender's signature (15)
No(s). of licence(s)	No(s). of certificate(s)	No. of invoice	

Figure 16 CN23 customs declaration form (the Royal Mail version)[66]

The final postal logistics phase is delivery. Swiss Post offers multiple delivery option for its private customers and business clients. Delivery to private mailboxes is still the most common method for letters and small parcels. When an item is too big to fit into a mailbox, a mailman may ring the recipient's doorbell and hand over the item personally. If the recipient is not at home, the mailman leaves a collection note that advises the recipient to pick up the item from a post office, typically the one nearest to the recipient. The postman may also leave the parcel (not

[65] A pro-forma invoice is a document indicating the seller's commitment to sell the imported goods to the buyer at specific price and terms

[66] The CN23 customs declaration form is used to declare letter-size items (< 2kg) worth more than 700 CHF. Below the 700 CHF limit, the sender can use a simpler CN22 customs declaration form.

requiring the recipient's signature) at the front door if the recipient has signed a delivery authorization. For certain mail products, the recipient may order a second delivery for free or against a small fee. If the item requires the recipient's signature or includes the cash on delivery (COD) service, the recipient must go to a post office. Clients, who prefer not to receive their parcels at home, can order their parcels to one of the Pick Post locations that are often situated at gas stations, kiosks and railway stations across the country. Also, clients can buy the Swiss Post box service to receive digital scans of their physical mail to an electronic mail box. The clients can also rent one of the thousands P.O. boxes, often situated in the proximity of post offices, or they may set a poste restante address at a post office counter.

5.3. Postal security domains

This section demarcates and characterizes domains of postal security management, areas of security activity that employ different security solutions, are driven by various motives and are regulated by specific rules. The security domains define the modern postal security management and shape the cross-border service as a whole. The domains defined and discussed here also set the basis for the case study analysis of the next chapter.

5.3.1. Export border controls

Export border controls count as one of the domains of postal security management. As mentioned earlier, foreign-bound Swiss postal items undergo export border formalities before exiting the Swiss territory. Sometimes, Swiss customs control postal exports for contraband and security threats. However, the representatives of Swiss customs highlighted that the main purpose of the export border formalities is to raise data for trade statistics. Another important purpose of the export controls is to fight curb trafficking and terrorism. To meet to security goal, Swiss customs sometimes control exported postal traffic for explosives and other security threats, dual-use goods, war material, drugs, cash, and cultural artifacts. Fiscal contraband is not an issue because Switzerland does not levy taxes or duties on exports. The risk of smuggled dual-use and military goods are a key export control concern for Swiss customs for reputational and diplomatic reasons (see Box 7).

Swiss customs assess risk levels of exported postal items and consignments based on information they receive from Swiss Post. This set of data comprises mainly item-level export declarations and consignment-level exit notifications. Tactical intelligence on immediate security threats is also used in the risk assessment whenever available. Although the customs assess risk levels of outbound postal consignments systematically, customs experts and managers at Swiss Post suggest that only a fraction of postal exports get inspected physically. The seemingly lenient export border controls stem from the fact that Swiss customs prefer to focus on goods entering rather than leaving the Swiss territory (after all, one of the Swiss

customs' key roles is to protect the Swiss people and economy from external threats). The second reason for the relatively infrequent export inspections is that the postal service is only a minor channel for illegal exports. "If you compare the risk of small envelopes to the risk huge trains and trucks leaving Switzerland, you concentrate your resources there where you think the risks are the biggest," a supply chain security expert from Swiss customs remarks. In principle, under the WCO's SAFE framework,[67] foreign authorities could request Swiss customs to inspect outbound postal shipments for security threats already at the Swiss territory. However, such requests are rare.

"It's very important for Switzerland that some countries and organizations don't get dual-use goods or something that could be a threat to the global security," a tax specialist from Swiss customs points out. Switzerland respects the United Nations' resolutions on trade sanctions and embargoes to sanction hostile or "non-cooperative" states, stateless organizations, and individuals. As of 24th January 2013, Switzerland had imposed sanctions against 17 states including North Korea, Libya, Somalia and Syria and numerous non-state organizations including the Taliban regime and the Al-Qaeda. Switzerland is also a member of several multilateral trade control regimes (see Table 30) that aim to restrict exports in certain dual-use and military goods, technologies, and materials. Recent failures to enforce export controls put Switzerland in an embarrassing light at international political arenas. In 2010, Swiss arms exports to Qatar eventually turned up in Libya. In 2012 Swiss-made hand grenades found their way to Syria via the UAE. Thus, to avoid diplomatic ramifications, the Swiss customs verify meticulously legality of all Swiss exports in dual-use and military goods through examination of licenses, permits, and end-user certificates. It should be remembered, however, that the postal channel lends itself poorly to transportation of relatively bulky dual-use goods and munitions.

Box 7 Importance export controls of dual-use and military goods

Export-control regime	Purpose	Members
Australia Group	Identification and control of exports contributing to development of biological or chemical weapons.	41
The Nuclear Suppliers' Group	Prevention of proliferation of nuclear weapons without hindering international trade and cooperation in the nuclear field for peaceful purposes.	46
The Missile	Prevention of proliferation of unmanned delivery systems	34

[67] "At the reasonable request of the receiving nation, based upon a comparable risk targeting methodology, the sending nation's Customs administration will perform an outbound inspection of high-risk containers and cargo, preferably using non-intrusive detection equipment such as large-scale X-ray machines and radiation detectors."

Technology Control Regime	capable of delivering weapons of mass destruction.	
The Wassenaar Arrangement	Promotion of transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.	41
The Chemical Weapons Convention	Elimination of an entire category of weapons of mass destruction by prohibiting the development, production, acquisition, stockpiling, retention, transfer or use of chemical weapons	188 signed and ratified; 2 signed.
The Biological Weapons Convention	Prohibition of the development, production, acquisition, transfer, retention, stockpiling and use of biological and toxin weapons	167 signed and ratified or acceded; 12 signed.

Table 30 Main multilateral export-control regimes

5.3.2. Airmail security & safety

The modern airmail security regime has been developed fast over the past four years largely due to the attempted mid-air bombings in October 2010, so-called Yemen bomb plot. To retell that story briefly, the bomb plot started to unfold when a double agent tipped Saudi-Arabian intelligence that al-Queada terrorists had shipped two parcel bombs from Yemen to the US via the express courier service. The Saudi intelligence forwarded the tracking numbers of the suspected explosive devices to their Western colleagues who ordered interception of the bombs at transshipment points in England and Dubai. In England, an elite bomb squad did not first recognize anything suspicious when they screened the suspected parcel at the East Midlands airport, nearly 200 km to the northwest from London. "It looked like a printer cartridge to us – there was no wires or anything," recounts a WCO's veteran customs expert and air cargo specialist. "But of course, what the cartridge did contain was explosive that current technologies couldn't detect." Later laboratory tests revealed that each parcel contained 300 to 400 grams of PETN, military grade plastic explosive, wirings, and a detonator hidden inside a computer printer's toner cartridge. The bombs were so meticulously concealed that they had not only passed the standard air cargo and safety screening but also the special screening of the bomb squad. Because the parcel bombs had travelled onboard two air freighters and three passenger planes before their interception, the bombs could have blasted one of the airplanes into pieces in Lockerbie-style mayhem. Figure 17 below illustrates flights and routings of the two explosive devices.

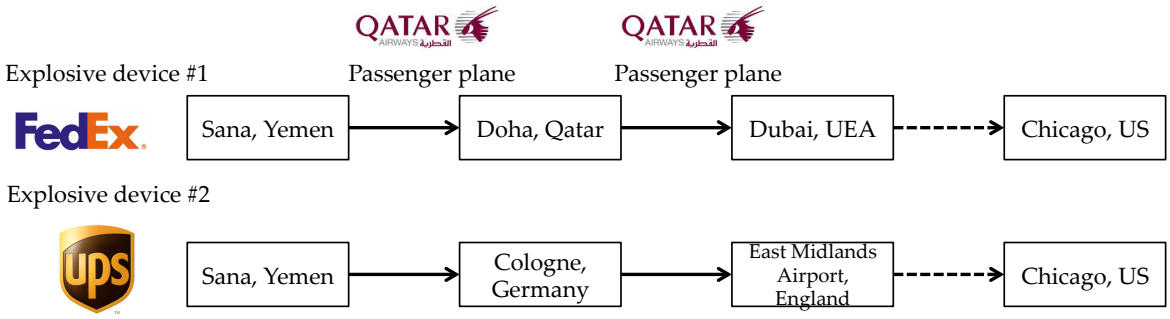


Figure 17 The Yemen bomb plot – routing of two the printer cartridge bombs

In the immediate aftermaths of the events, aviation security authorities in the US and many European countries stopped accepting freight shipments from Yemen. Germany also cancelled all passenger flights from Yemen for more than two weeks. "As often happens in these situations," the WCO's air cargo specialist remarks, "the first reaction was stopping anything coming from this part of the world – any plane for any reason." Eventually, once the precautionary stoppage was ended, new unprecedentedly stringent security requirements entered into force, disrupting the airmail service further. The US Transportation Security Administration (TSA) introduced the most draconian rules: any mail originating or transiting through Somalia or Yemen was banned, as well as printers or printer toner cartridges. Moreover, parcels originating from any business partners had to be screened up to high-risk screening standards piece by piece if such shipment did not accompany a tendering statement. The new regime disrupted seriously international postal logistics, causing Posts worldwide to accumulate huge backlogs of US-bound shipments. The statement of the UPU illustrates best the situation caused by the new airmail security measures:

> "The measures […] forced the national Posts of UPU member countries worldwide to change their operational procedures overnight. Some Posts stopped accepting or delayed US-bound mail items, including courier products, and faced higher transportation costs and the shutdown of major mail transit hubs." (UPU statement, in Post & Parcel 2012)

Annoyed and surprised about the turn of events, the postal industry reacted to the US regime with a barrage of criticism, calling the measures superfluous and impractical. To pacify the situation, the US authorities eventually relaxed the stringent air cargo and mail security measures, which enabled the Posts to start slowly clearing the backlog of the US-bound mail. In April 2011, to lower the risk of future security-related disruptions to the mail service, the UPU assigned an ad-hoc inter-committee security group, a cooperative of UPU, ICAO, IATA, WCO, and TSA, to draft baseline security requirements for the postal sector. The international requirements were thought to reduce the need for very stringent emergency measures in response to possible future terrorist threats in the airmail channel. Not long after, the work of the committee resulted in two standards, one laying down general rules for postal security (S58)

and the other specifying minimum security standards airmail security (S59). The 25th Universal Postal Congress, held in Doha in Qatar in September/October 2012, opted for making the both security standards mandatory for all UPU members. The congress also updated the ICAO-UPU memorandum of understanding on the airmail security and established a joint contact committee on the topic. Later in July 2013, the 17th amendment to the Annex 17 of ICAO's came applicable, introducing concept of high-risk cargo and mail and more stringent screening measures, and consignment security declaration into the global legislation.

The overall purpose aviation security, the ICAO's annex 17 states, is to safeguard civil aviation from "acts of unlawful interference," including mid-air bombings, sabotage, skyjacking, and hostage taking. In the air cargo and mail domain, the scope of the security threats reduces to assembled explosive and incendiary devices that can destroy aircrafts if hidden inside airfreight. To mitigate the risk of explosives entering cargo holds, air cargo and airmail are generally screened with X-ray or other techniques prior the freight is loaded onboard. The screening targets also safety threats that encompass otherwise legitimate goods – matches, perfumes, lithium batteries, and so forth – that may endanger flight safety due to their hazardous properties. Recall from the previous chapter that even if both safety and security threats are both capable of destroying planes, the threats are fundamentally different: security threats arise from deliberate hostile action whereas safety threats occur due to negligent and/or unintentional behavior. Unlike bombs and other security threats, safety threats rarely cause problems during flight even if screening fails to recognize them and they end up aboard.

Switzerland is fully integrated into the EU's aviation security regulatory area[68] under the Agreement of the European Community and the Swiss Confederation on Air Transport (L 2002 114/73). The agreement states that Switzerland must design and implement national aviation security and safety programs as EU-level directives, regulations, and decisions dictate. The EU's current regulatory framework, as relevant for airmail, comprises the framework regulation 300/2008 (chapter 6 of annex), the supplementing regulation 272/2009 (part F) and the implementing regulation 185/2010 (chapters 6 and 11). Other relevant regulations 1254/2009 and 72/2010 grant derogations from security requirements for small airports and provide specifications for the Commission's compliance inspections. On top of the main regulations, a series of confidential decisions of the European Commission lay down technical provisions for security compliance. The confidential decisions are shared only with "appropriate" national civil aviation authorities (CAAs) that in turn disseminate the decisions further to the industry on a need-to-know basis. In Switzerland, the Federal Office of Civil Aviation (FOCA) is the appropriate civil aviation authority. Its responsibilities include development, implementation,

[68] As of September 2014, the EU aviation security area covers the 28 EU member states, Iceland, Norway, and Switzerland.

and monitoring of the confidential Swiss national aviation security programme so that it reflects the EU's regulatory framework.

The EU air cargo security rests on a principle that all cargo and mail must be screened up to the EU standards prior loading onto an aircraft that takes off from or is bound to any EU airport. However, one exception to this principle is cargo and mail coming from a "secure supply chain" that can be conditionally loaded aboard an aircraft without (additional) screening at the airport. Secure cargo and mail originate from certified known consignors (KCs) or account consignors (ACs) and is handled by a chain of certified regulated agents (RAs) from the source to the aircraft's cargo hold[69]. Another special exception to the 100% screening principle is the diplomatic mail that is exempted from security and safety checks under the article 27 of the Vienna Convention on Diplomatic Relations.

The security screening is technically defined as the use of "technical or other means" for detection of explosive or incendiary devices among air cargo and airmail shipments. The implementing regulation 185/2008 states that mail shall by be screened by a method, or a combination of methods, that are most likely to detect explosive and incendiary devices. Besides, the applied screening methods "shall be a standard sufficient to ensure" that mail items are safe. Against the common believe, there are many other screening methods besides the "X-raying." In fact, the supplementing regulation 272/2010 allows regulated agents to screen airmail with eight methods: hand search, visual check, X-ray equipment, explosive detection systems, explosive detection dogs, explosive trace detection equipment, simulation chamber and metal detection equipment (the last-mentioned was introduced in the amending regulation 297/2010). The confidential decisions of the European Commission set performance and testing criteria for the application of these screening methods. The post-Yemen EU aviation security regulations introduced the concept of high-risk cargo and mail (HRCM), a type of cargo that must be screened in line with special instructions. The regulation 1082/2012 considers all "consignments which originate from or transfer in locations identified as high risk by the EU or which appear to have been significantly tampered with" as high-risk cargo and mail. Though not public information, it fairly safe to assume that the high-risk origins and transfer sites refer to Somalia, Yemen, and other unstable countries presumed to harbor terrorism. The HRCM designation means that regulated agents must screen such consignments "in line with special instructions" which that the European Commission has specified in confidential decisions. HRMC screening requirements are likely include multi-method piece-by-piece screening that is slower but more thorough than the standard screening.

[69] It is important to note that although no legal restrictions prevent European Posts from benefiting KC or AC programs, the postal sector currently ignores them.

In Switzerland, Swiss Post is responsible for arranging airmail security and safety screening. The company has, however, outsourced the screening operations to specialized security services, as the subcontracting is a less expensive alternative than "building and maintaining in-house airmail screening expertise," as a Swiss Post's manager put it. The screening operator sometimes screens relatively small postal items collectively in mailbags or other receptacles, without taking individual items out of the mail aggregate. Heavy and thick parcels and small packets, which travel separately outside receptacles, are often screened individually piece-by-piece. When screening for security threats, the assembled explosive and incendiary devices, the X-ray screening operators look for suspicious wirings, explosive charges, detonators, and piercing projectiles such as nails, screws, or airsoft pellets. The less rays penetrate or scatter from the inspected matter, the darker the substance appears on the operator's screen. Because the explosive substances commonly absorb atypical large amounts of radiation, most explosives appear as black boxes on the operators screen. The operators try to resolve "black alerts" by screening the inspected objects from different angles, or by using complementary screening techniques such as dogs and trace detectors. As the last resort, the operator calls a bomb squad. To date, no explosives have been detected in the Swiss airmail traffic, or at least the interviewees were not aware of or willing to talk about such incidents. Safety contraband is much more commonly encountered in the airmail screening than security contraband: screening operators remove multiple hazardous articles from postal items every day, mainly perfumes, aerosols, lithium batteries, and matches.

When the airmail is screened and secured, the security service provider issues a consignment security declaration (CSD) that specifies the security status of the consignment, its audit trail through security controls, reason why the security status was granted, and the identifier of the regulated agent responsible for the screening (see Figure 18 for details). The EU legislation recognizes three security statuses: SPX = secure for passenger and all-cargo aircraft, SCO = secure for all-cargo aircraft, and SHR = secure for passenger and all-cargo aircrafts in accordance with high-risk cargo and mail (HRCM) requirements. Once issued after the screening, the security declaration accompanies the consignment over the duration of the flight and it must be made available for authorities on request. The aviation industry, internationally represented by IATA, is currently developing a digital equivalent of the consignment security declaration, the electronic cargo security declaration (e-CSD).

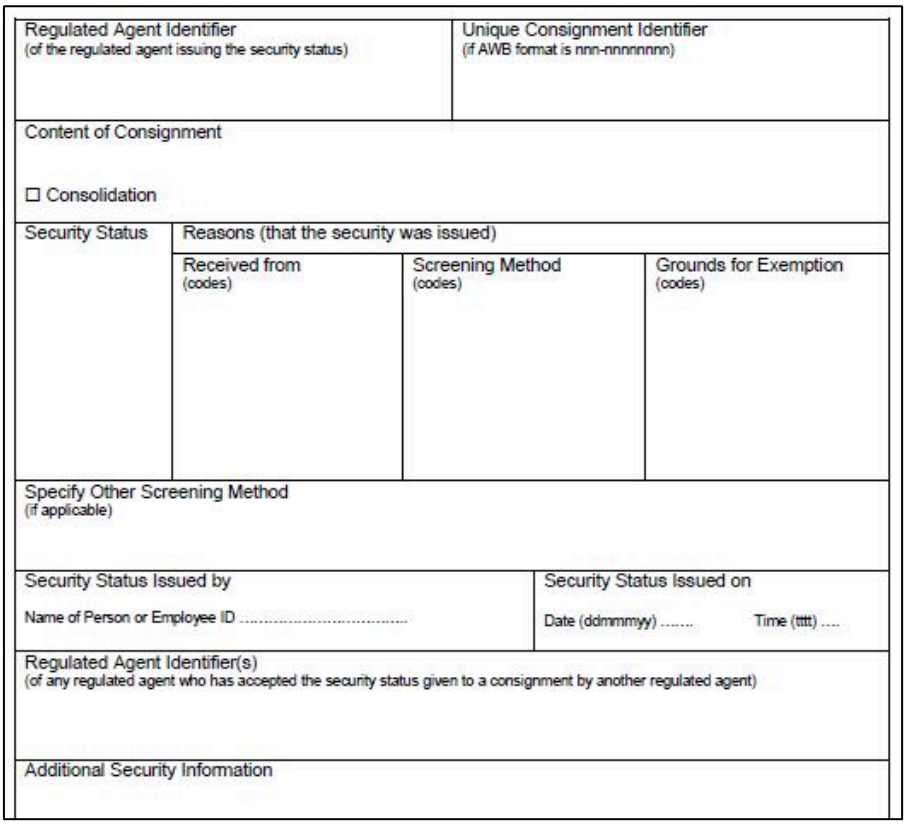


Figure 18 Consignment security declaration (CSD)

The regulated agents like Swiss Post are also responsible for protecting the screened airmail shipments from unauthorized tampering until they are loaded into airplanes' cargo holds. Three elements – sealing, accredited handlers, and physical security – contribute to the post-screening integrity. After the screening, Swiss Post's employees commonly pack airmail into air cargo containers, seal the containers, and hand them over to certified air cargo handlers who take care of the loading aboard. "We seal airmail containers, and ground handlers check the seal's integrity before they load the containers onboard," Swiss Post's security manager explains. "If the seal is broken, the airmail shipment must be screened once more." If the air cargo containers are not used, and airmail is loaded as in receptacles as loose cargo, the receptacles themselves are sealed. During and after the screening, only accredited regulated agents and their trained employees, whose backgrounds aviation authorities have vetted, can handle the airmail. Physical security measures at the airport – fences, gates, guard patrols, and access control systems in particular – prevent uninvited people from entering airmail handling premises.

Only the regulated agents are allowed to screen airmail, grant security statuses for airfreight consignments, and handle identifiable, secured airmail. Air carriers, ground handling agents, and logistics service providers, such as posts, may apply for site-specific regulated agent

statuses. The applicants of the regulated agent, the known consignor, or the account consignor certificates need to develop and implement an internal security program that meets the requirements of the framework regulation 300/2008 and its implementing acts. Besides detailed security measures, the program should describe an internal quality control mechanism for self-compliance monitoring. The applicant's legal representative, or a person responsible for security, must also sign and submit a "declaration of commitments" as part of the application. Later in the accreditation process, the national civil aviation authority (FOCA in Switzerland) examines the security programme and visits the applicant's premises to ensure the proper implementation of the security measures and the self-compliance mechanism. If the auditor decides to grant the status to the applicant, he registers the new regulated agent into the European Commission's "database of regulated agents and known consignors".

In Switzerland and elsewhere in the area of the EU aviation security regime, the formal compliance monitoring system relies on national quality control programs, complementary Commission inspections, and self-compliance mechanism of the regulated agents. The authority should re-evaluate the compliance of the regulated agent at least every five years. In addition to the scheduled audits, the European Commission, together with national civil aviation authorities, may inspect regulated agents together with national authorities without prior notification. The inspections and security audits may be comprehensive or focus on certain aspects of operators security programs. In specific "tests," that simulate hostile attacks, authorities send inert bomb replicas and other threat items by mail to evaluate performance of the airmail screening system. The authorities have mandate to provide advice and support, issue formal warnings, give enforcement notices, impose administrative sanctions, revoke the status of regulated agent, or start legal proceedings if regulated agents fail to meet satisfactory standards[70]. Also air carriers audit their clients, especially in high areas. We don't really have resources to do every station every year," a security manager from SWISS says. "We are not focusing on countries and stations where security already is at a high level." Audits clearly concentrate on least developing parts of the world. If SWISS detects substandard security practices, they resolve the problem by pressuring their suppliers to rectify the problems. Breaking the contract is the last resort, the SWISS' security manager says. "Security is paramount, but we want to do business, too." Overall, Swiss Post and its security service providers typically face one or more compliance audits a year at its two airmail handling exchange offices in Geneva and Zurich.

[70] ICAO runs its own "Universal Security Audit Programme" (USAP) that monitors compliance of the ICAO's contracting countries with the provisions of the requirements of the Annex 17 of the Chicago Convention. However, since the signing of "Memorandum of Cooperation" between the European Community and ICAO on aviation security audits and inspections, the European Commission and ICAO authorities have no longer been carrying out duplicate aviation security audits.

Quite recently, largely motivated by the Yemen bomb plot, the European civil aviation community has taken major leaps towards the "one-stop-shop" security. The EU regulation 859/2011 forces air carriers operating from third country airports to comply with the EU's 100 % screening and "secure supply chain" rules. The carriers must apply for a designation, called Air Cargo or Mail Carrier operating into the Union from a Third Country Airport (ACC3), for every third country airport from where they fly into the EU, Norway, Iceland, or Switzerland. Because of this new legislation, all airmail shipments arriving at the Zürich or Geneva airports should have already been secured up to the EU standard at the origin or one of the possible transfer stations. Therefore, in principle, Swiss Post does not need to re-screen airmail that transfers in Switzerland en route to any EU member state, Norway, or Iceland. Another important milestone was achieved when the EU and the US agreed to recognize each other's air cargo security regimes in June 2012. As soon as the agreement entered into force, there was no need to re-screen US-bound airmail at European transfer stations. However, despite the impressive advancements in regulating air carriers operating into the EU and mutual recognition agreements between the US and the EU, re-screening is still a commonplace in Switzerland and other European countries, which airports serve as transfer locations for international airmail traffic. In Switzerland, the re-screening takes always place when Swiss Post deconsolidates airmail consignments and assigns individual shipments to several connection flights (so called open transfer). If Swiss Post's handlers only transfer the containers and the mailbags to the connecting flight without breaking the sealing of the consignment (so called closed transfer), the re-screening takes place only if the airline operating the connecting flight asks Swiss Post to do so. The airlines' requests for extra screening can be based either on the airlines internal policies or the air cargo security regime of the destination country. Further efforts for one-stop-shop aviation security are urgent. "Screening must be done at the origin because why should the second flight be different from the first flight," the security manager from SWISS asserts. "There are also passengers on the first flight. Everything, that needs to be done, gets done at the origin and before the airmail gets loaded on our flight."

Another key foreseen reform in the airmail security domain is the extensions of the advance electronic information to cover some segments of the postal traffic (see background of the Swiss-EU collaboration on customs security matter in Box 8). The current EU's customs security legislation exempts "letters, post cards and goods moved under the rules of the Universal Postal Union Convention" from the provision[71] of the item-level advance electronic information (AEI) datasets, the entry and exit summary declarations. This exemption, however, is going to be revoked for certain categories of postal items when the new Union Customs Code eventually supersedes the current Community Customs Code (and "recasts" the Modernized Customs

[71] Art. 181c and 592a

Code)[72]. More importantly, besides the revocation, the draft legislation is going to require Posts to lodge the exit and entry summary declarations before postal items are loaded aboard airplanes. This new *pre-loading* principle is a crucial difference between the old and the new legislation as it allows authorities to use the AEI dataset for aviation security purposes. Let me clarify the previous statement. The current, "old" legislation advocates the *pre-arrival* principle that mandates lodging of entry summary declarations at the time of takeoff for short haul flights (< 4 hour flight time) and 4 hours before arrival for long haul flights (> 4 hour flight time). The new legislation introduces an earlier deadline for the lodging of the entry (and exit) summary declaration that allows the customs to carry out risk assessment and instruct possible extra security measures (e.g., more intense screening, request additional information, or deny loading) before the items are loaded aboard an aircraft and take a flight. The lodging of the AEI information supports risk-based screening of airmail shipments and "adds another layer to the security risk mitigation," as the security manager of SWISS remarks. He highlights that the aviation industry "very much supports" the new pre-loading AEI scheme "because it gives the shipment a risk classification" that allows airmail screening operators to focus more attention on the most risky shipments. The focused attention means that the high-risk airmail items would be screened up to the high-risk cargo and mail (HRCM) requirements, as suggested in the regulation 859/2011 and specified in a confidential decision of the European Commission. The HRCM screening, most likely, involves piece-level inspection that is more intense and time-consuming than the standard airmail screening. Table 31 below illustrates the main differences between the old Community Customs Code (CCC) and the new Union Customs Code (UCC) in terms of airmail security.

Regime	Community Customs Code	New Union Customs Code
Target	Threats to aviation security (IEDs & IIDs)	General security threats & contraband
AEI data elements	Shipment data & transport data	Shipment data & possible transport data (dual filing)
Deadline for data submission	"Wheels up" for < 4 hour flights / 4 hours before arrival for > 4 hour flights.	Before loading "as soon as possible"
Targeting approach	Rule-based	Score-based

[72] The European Commission decided to recast (i.e., amend) the Modernized Customs Code so that the new customs legislation would be split between implementing and delegated acts as the new Lisbon Treaty mandates and so that the European Commission would have time to build IT capability and to consult the trading community and national customs administrations (COM 2012/64).

Table 31 Key differences between the Community Customs Code and the Union Customs Code

The EU legislation on the customs security has been evolving rapidly since the "9/11" attacks in 2001 that put the security of the global supply chain into a spotlight. In 2003, the European Commission set the general policy for the EU customs security in the communication (2003/452). A few years later, the so-called Customs Security Amendment (648/2005 and 1875/2006) translated the policy into legal requirements. The amendment introduced electronic pre-arrival and pre-departure declaration requirements for most cargo traffic crossing the EU border, the EU Authorized Economic operator (AEO) program, and the common risk assessment and uniform criteria for identification, and control of high security risk cargo movements. It was soon recognized that the Customs Security Amendment would hinder the Swiss-EU trade and disrupt the transit traffic through the landlocked Swiss territory, which is surrounded by EU member states (except for Liechtenstain). "We would have had a huge problem without the agreement: millions of shipment should have been pre-announced at our borders," recounts a supply chain security specialist from Swiss customs. To ensure the smooth trade flows also under the amended rules, Swiss and EU authorities started negotiations on integrating Switzerland into the EU's customs security area. In June 2009, after nearly two years of negotiations, the EU and the Swiss officials signed the Agreement on Customs Security and Facilitation[73] and annexed it into the existing bilateral Agreement on the Carriage of Goods, that had already been defining rules for simplified customs formalities for cargo traffic between the EU members and Switzerland. Since the agreement on Customs Security and Facilitation entered into force 1st of January 2011, Switzerland has been following the EU's customs security regime. "We are [now] fully integrated into the security schemes and the security area of the EU – we are like the 28th member[74]," the supply chain specialist from Swiss customs points out. "We are not allowed to have a different level of security in Switzerland, or otherwise we would be a hole in their security scheme."

The Agreement on Customs Facilitation and Security builds on three building pillars of the EU's Customs Security Amendment[75] (648/2005): the pre-arrival and pre-departure declarations, the EU AEO program, and the EU-level common security risk assessment. The introduction of the pre-arrival and pre-departure declarations was the biggest implication for the Swiss traders who needed to start lodging entry and exit summary when they traded goods with non-EU "third" countries[76]. The agreement's second pillar introduced the Swiss AEO-S program, and allowed AEO-S status holders to use a reduced dataset in the entry and exit summary declarations and get (conditionally) notified of customs security inspections[77]. The third pillar, the EU-level common risk assessment, meant that the first customs office of entry into the EU became responsible for security risk assessment and inspections for imported goods

[73] SR 0.631.242.05 in the Swiss legislation. OJ L 199 in the EU legislation.

[74] Note that the interview took place before 1st of July 2013 when Croatia become the 28th EU member state.

[75] It is important to note that the update concerns only *customs security*, not duty and tax collection, trade controls, or other customs matters.

[76] Besides the 28 EU member states, also Norway is part of the EU's customs security regime.

[77] As 10 July 2014, there were 46 AEO-S certified Swiss companies, including TNT-Swiss Post, the Swiss Post's express courier subsidiary.

regardless of their final destination in the EU customs security area. "If a postal shipment arrives by sea, one of the EU customs might do security checks for us and we would consider that ok," a supply chain security experts from Swiss customs clarifies. He adds that because long distances and the urgent nature of the postal traffic, postal items from the non-EU countries enter directly Switzerland by airplane, and thus Swiss customs risk assess and inspect incoming airmail for security risks.

Box 8 Evolution of the EU-CH collaboration in the customs security area

5.3.3. Transit border control

International postal shipments often transit through one or more countries on their way to the final destination. Customs and other border control authorities may control transiting postal traffic for contraband or security threats, but they rarely do so. The main reason for the lack of the transit controls is that the authorities prefer to focus their limited resources to control mainly imports, secondarily exports, and only thirdly transits. Another reason is that authorities in the transit countries receive only consignment-level information on the postal transits, and this general information does not lend itself to effective risk assessment. A third reason for the lenient transit controls is the fact that international conventions governing the cross-border exchange of postal items discourage customs and other border agencies from intervening with the transiting postal traffic:

> "Postal items shall not be subject to Customs formalities whilst they are being conveyed in transit." (Revised Kyoto Convention, Specific Annex J, Standard 10)

> Each member country to shall ensure that its designated operator forwards, always by the quickest routes and the most secure means mail items, which are passed to them by another designated operator. (UPU Convention, Article 4, paraphrased)

The apparent leniency of the transit controls, however, does not exclude the possibility that transiting postal items might attract law enforcement scrutiny and face inspections. Inspections indeed occur when the authorities in the transit countries receive a piece of tactical intelligence, typically a phone call from a trusted source, indicating that something illegal and/or dangerous is about to move through their jurisdiction. For example, it was timely tactical intelligence – tracking numbers of two explosive express courier deliveries – that allowed authorities to intercept and defuse bombs on the way from Yemen to the US in late October 2010. In 2013, thanks to a critical piece of tactical intelligence, Swiss customs seized around 5000 counterfeit watches from airmail parcels that were transiting through Switzerland en route from Greece to Spain and Portugal.

5.3.4. Pre-declaration import border controls

All foreign-origin postal items that enter the Swiss territory and that are sent to Swiss addressees are subject to import customs formalities. Swiss customs may decide to control postal imports immediately as soon as postal consignments arrive at exchange offices. This takes place before the postal items are unloaded, and before the customs have received formal import declarations. In such so-called pre-declaration border controls the customs target security threats and contraband that are illegal no matter what information is eventually provided in the formal, legally binding import declarations. A risk assessment specialist from Swiss customs tells that the pre-declaration controls target primarily security threats, including "explosives, weapons, and radioactive items" and secondarily narcotics, counterfeits, and CITES goods. Swiss customs select postal consignments to controls based on results of risk assessment. The risk assessment is done based on consignment-level information, as currently the customs have no item-level information at hand before the import declarations are lodged. Tactical intelligence is another input to the risk assessment, whenever available. In the actual risk assessment, all available information and intelligence is compared against high-risk indicators and risk profiles to identify consignments that pose the highest risk and thus call most urgently customs officers' attention. Because of the risk assessment, a consignment from a known cocaine source country gets more frequently inspected with drug sniffing dogs than an average consignment. If a consignment gets selected to the pre-declaration controls, the customs officers send a "Do Not Unload" message to Swiss Post. This message means that when the selected consignment arrives at one of the Swiss Post's exchange offices, it must be left untouched until a team of customs officers come and inspect its contents with dogs, X-ray equipment, material trace detectors, or whatever technique most fit for the purpose. However, if the team of officers does not start the inspection within 15 minutes after the arrival of the consignment (so-called intervention period), Swiss Post's people may go ahead and unload the consignment and start declaring the items to the customs one-by-one. At the time being, the pre-declaration controls are relatively rare. The controls take place "a few times a year," Swiss customs' risk assessment specialist points out. He hurries to add that Swiss customs are anyhow doing "more and more" pre-declaration controls in the postal channel. Despite the relatively low frequency of the pre-declaration controls, the controls have resulted in large seizures. In 2009, for example, a pair of sniffer dogs detected two kilograms of cocaine at the mail exchange office of the Zurich airport.

The frequency of pre-declaration controls increases significantly during periodic law enforcement campaigns. For instance, as part of the INTERPOL-led operation Pangaea, people from Swiss customs and SwissMedic (the Swiss Agency for Therapeutic Products) inspect imported postal parcels intensively for illegal medicines and medicinal instruments. During the eight-day-long operation Pangaea V in 2012, Swiss authorities opened and examined 750 postal

packages and confiscated nearly half of them due to illegal contents. The seizures prompted SwissMedic (2013) to estimate that approximately 20000 shipments of illegal mail-order medicines enter Switzerland every year[78]. The annual operation Pangaea is the main law enforcement campaign in the postal channel, though Swiss customs participate campaigns as well, such as the operation "Colosseum" that fights illegal trafficking in cultural artifacts.

The Swiss Federal Customs Administration, the primary border control agency for merchandise trade in Switzerland, enforces the customs law[79] and around 150 other non-customs laws and regulations at the Swiss borders. The customs' main responsibilities include the collection of duties, fees, excise taxes and VAT from the international traffic; protection of the Swiss population, economy, and the environment; contribution to the national and international security; and collection of statistics that allow calculation of foreign trade balance and projection of future tax and duty revenues. The customs' priorities, goals, and performance measures are defined in a four-year mandate that the Federal Department of Finance co-creates with the customs and other government agencies that have an interest in the cross-border traffic, including the international postal traffic.

Box 9 Swiss customs in a nutshell

5.3.5. Post-declaration import border controls

After the possible pre-declaration controls, the Swiss Post's customs brokers unload the postal consignment and start declaring parcels and letters to Swiss customs item-by-item. The next controls take place after the declaration is done. "We need a legally binding customs declaration before it's meaningful to inspect," Swiss customs' supply chain security specialist says and explains that customs detect fiscal contraband by comparing the declared data against the physical documents and contents of the shipment. "Without the declaration we don't know what to expect." After the customs have received the legally binding import declaration data, the post-declaration border controls can take place. The customs' post-declaration controls target mainly fiscal contraband, counterfeits, narcotics, and security threats. In addition to customs controls, the SwissMedice targets illegal medicines and medical devices, and the Federal Food Safety and Veterinary Office CITES goods.

Recall from the previous section that Swiss Post holds an authorized consignee status that allows the company to benefit from streamlined customs procedures. Most importantly, the status enables Swiss Post to declare imported postal items from their inland mail exchange

[78] At the global level, authorities participating the Pangaea V examined around 130.000 postal parcels and seized medicines and medicinal products worth almost 10,5 million.

[79] RS 631.0

offices instead at the Swiss borders[80] or at separated customs offices. The status also allows the Swiss Post's customs brokers to use simplified import declarations to report majority of postal items to the customs. For instance, items containing gifts worth less than 100 CHF or commercial goods worth less than 62 CHF, if the contents are not subject to special regulations such as import permits, licenses, quotas, or special duties. In some cases, the Swiss Post's brokers use traditional stamps (see Figure 19) to declare letter-post items that are not subject to taxes or duties. As regards to small letters and postcards, which contain personal correspondence, no import declaration is required. Otherwise, the customs brokers fill in electronic item-level import declarations online, using the Swiss customs' "e-dec" web interface. The customs electronic software crosschecks the declaration data for inconsistencies and prompts corrections before the broker submits the legally binding declaration to the customs. This plausibility check, for example, verifies whether the declared product descriptions and quantities correspond the declared weight and value. The Swiss Post's customs brokers are responsible for any mismatches between declared information and the actual contents, so they have a strong incentive to comply with customs instructions. "If they didn't do their job properly, we could withdraw their authorization as an authorized consignee," the supply chain security expert from Swiss customs explains. "We could also decrease or increase the number of controls we do." To avoid mistakes, it is a commoplace that during the declaration process, the customs brokers open some postal items to verify contents. And if the brokers encounter anything suspicious, potentially illegal, they are obliged to report their superiors or directly customs officers.

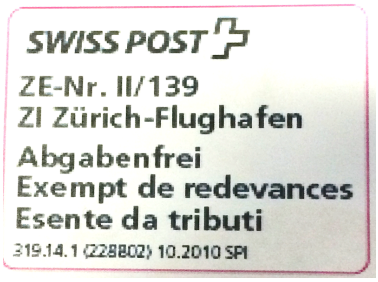


Figure 19 Customs declaration stamp (only for imported letter-post items)

After the brokers have lodged the electronic import declarations of those items that are not eligible for the simplified customs declaration[81], the Swiss customs' automatic risk assessment engine compares the dataset against a set of predefined high-risk indicators and profiles as well

[80] Swiss Post can declare international surface postal items from their Zurich-Mülligen mail exchange office, which is located nearly 20km away from the Swiss-German border.

[81] Due to the stamp declaration, Swiss customs do not receive electronic item-level information on standard non-dutiable items, which categorically inhibits automatic risk assessment for this segment of postal traffic.

as calculates a risk score for each declared item. Swiss customs has more than twenty high-risk indicators and profiles to risk assess the postal traffic. "The country of origin is the most important high-risk indicator in imports," the risk assessment specialist from Swiss Customs explains. For example, counterfeit traffic to the European Union is strongly associated with certain source countries: cigarettes from China, UAE, and Moldova; clothes from China and Turkey; watches from China and Hong Kong; and medicines from China, India, and Hong Kong (EC 2012). High-risk indicators, other than the country of origin, include vague description of goods, missing or invalid return address, and inconsistencies between declared weight, quantity, value, and contents. "Typically, the less information you have, the riskier the shipment is," the Swiss customs' a supply chain security specialist generalizes.

The risk assessment engine blocks around 20% of parcels and letters and releases the remaining 80% of the postal items immediately to the national circulation. Again, customs officers must arrive and start inspecting the blocked shipments within another 15-minute intervention period or otherwise Swiss Post can proceed with the standard sorting and delivery procedures. If the customs officers show up, they examine the blocked items and associated documents. Drawing on their experience on typical traffic flows, concealment methods, and fraudulent documents, they select the most suspicious items for closer manual inspections. "After years of fieldwork, the officers know what to look for," the customs' tax specialist says. "It's the sixth sense of the customs officer that guides them to the right direction. […] How does the invoice look like? Is the routing strange?" The officers look for clusters of suspicious signs, relying on their intuition. For example, the signs suggesting presence of a mail bombs include unnecessary robust packaging, distinct smell, excessive postage, or stickers saying "do not X-ray" or "confidential," ticking noise, obtruding wires, oil stains, or declared contents that make detonators and wirings seem normal (e.g., "electronics"). Altogether, the customs officers examine roughly 20% of the blocked shipments, which accounts for 1% of the all imported postal items.

Swiss customs collect more than 24 billion francs in total taxes, duties, and other receipts from the cross-border traffic in general, across different modes of transport. In Switzerland duties are charged mainly by weight or unit whereas in most other countries duties are levied based on value (i.e., ad valorem). Product type and country of origin determine the applicable duty rate. As a member of many trade blocks, Switzerland collects lower or no duties from traffic coming from its preferred trade partners. The trade agreements have lowered duties rates and revenues across the world over the past twenty plus years. Today, in Switzerland and elsewhere, customs raise significantly less duties than value-added tax (VAT), excise, or other types of taxes levied on cross-border merchandise. The general Swiss VAT rate is 8%, although food, alcohol-free drinks, books and medicines are subject to the reduced 2,5 % VAT rate.[82] To determine the base value for VAT computation, one needs to add up the sales price, duties and excise, freight fees, insurance, and other possible handling fees. The Swiss customs collects excise taxes for example from imported alcohol beverages, tobacco products, and mineral oil.

Box 10 Calculation of taxes and duties for imports

Figure 20 summarizes the import control process from the perspective of the Swiss customs. The illustration exhibits the timing of information exchange and location of possible customs interventions in the import declaration process. It also shows how the Swiss customs conducts two different risk assessments to select postal shipments first for the pre-declaration controls and then for the subsequent post-declaration control.

[82]RS 641.20, Art 25

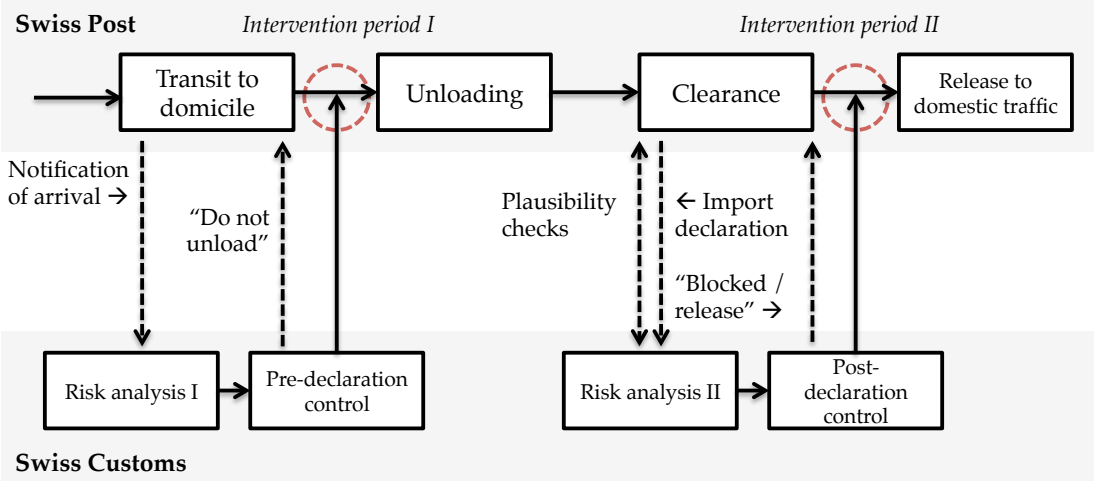


Figure 20 Summary of the overall import declaration process

5.3.6. Parcel bomb screening in the surface traffic

Except for the airmail, the law does not oblige Swiss Post to control any segment of the postal traffic for contraband or security threats. Otherwise it is the responsibility of customs, police, and other Swiss authorities to control postal traffic whenever needed. However, in spite of the lack of the legal obligation, Swiss Post controls imported surface parcels for explosives. These voluntary controls were set soon after March 2011 when a parcel bomb exploded at the office of Swiss Nuclear, in Olten, Switzerland, inflicting minor injuries on two office workers. The following police investigations revealed that the parcel bomb arrived by truck from Italy and went through the Swiss Post's exchange office in Mülligen before entering the Swiss postal system. It was also found that Swiss Post's customs brokers should have opened the parcel in a standard customs clearance process because the parcel was travelling without sufficient customs declaration information (i.e., poorly filled CN23 form). But because the brokers failed to follow the standard procedure for reasons unknown, the parcel passed the exchange office unopened and exploded eventually at the headquarters of the Swiss Nuclear. In response to the bomb incident, that almost lead to a fatal explosion in the exchange office, Swiss Post decided to start X-raying all imported parcels that get opened in the import clearance process and that arrive Switzerland by truck. The security screening is done with an X-ray machine at an off-site facility. "You lose one day in the X-raying process because all parcels, which have to be screened, are put aside and transported to the screening site at the end of the day," a Swiss Post's security manager explains. "Next day, the parcels come back and join the regular mail flow."

5.3.7. Police operations

Swiss police authorities can execute targeted raids, controls, or investigations virtually anywhere in the Swiss postal network. Typically, the police get involved in the postal traffic when mail gets stolen, letter or parcel bombs explode, or when narcotics or stolen goods are found in the postal system. It is important to understand, that the policing in the postal channel is far less systematic than the border controls or the airmail security screening. Rather, the police intervenes with the postal traffic only after a crime has already occurred or when there are reasonable reasons to assume that criminal activities are about to occur in the postal system. Most police activities in the postal network are triggered by tactical intelligence on prospective crime or information on recent crime incidents. Foreign police authorities might note their Swiss colleagues that a postal parcel with illegal contents is about to enter Switzerland[83] (the reason why the foreigners have not already intercepted the shipment is that they want to identify its recipient by letting the shipment pass through the postal system under surveillance and by observing who picks up the shipment eventually and what he does with it). Sometimes external informants, members of rival criminal gangs for example, tip the police off illegal postal traffic. Sometimes a key piece of intelligence is found during ongoing criminal investigations whereby police detectives collect evidence against suspects. A representative of the Cantonal police explains: "If we listen to phone calls of a suspect and he says, 'I have drugs for you,' we might think that he's going to send a parcel or deliver the drugs otherwise." Sometimes the police encounter illegal items by accident when the investigators open postal items addressed to a suspect[84].

Based on the the urgency and seriousness of the suspected crime, the police decide the most appropriate measures to deal with postal crime. In large mail theft investigations, the police may dedicate full-time detectives on the case. If someone receives dangerous or intimidating mail (e.g., bombs, hoax anthrax powder letters, or hate mail), his "future mail could go through our bomb squad," tells the representative of the Cantonal police. "And the common inquiry would follow: 'Do you have any enemies or problems with some people.'" In case of a drug delivery through the postal service, the police might carry out a controlled delivery, an

[83] The international collaboration between authorities works also to the reverse direction. "If we find drugs [in a US-bound postal shipment], we tell the US authorities the names of the sender and the receiver," the representative of the cantonal police states. The Swiss Post's manager explains the Swiss Post's role: "We don't inform the US police directly. When we find something [illegal], we inform the police. The Swiss police may inform the US police, and they may go after the sender."

[84] It should be noted that the police detectives must get an authorization from a prosecutor before they can start opening a suspect's letters and parcels systematically. According to the representative of the cantonal police, getting the authorization "is not usually a big problem" if the police already have reasonable evidence of the suspect's involvement in a grave crime. Petty crimes do not warrant the use of wiretapping, interception of mail, or other coercive, undercover monitoring techniques. "The limit for the grave offense is, for example, eighteen grams of one-hundred-percent cocaine and twelve grams of heroin," he exemplifies.

investigative technique whereby the police lets the illegal shipment to be delivered to the recipient under surveillance. "Once we got a drug shipment from Congo, toys stuffed with cannabis," a Swiss Post customs broker recalls. "The customs people came here and found 20 kg of cannabis inside the toys. They instructed us to let the shipment go through."

The controlled delivery is an important investigative technique that merits further attention. In a typical controlled delivery the police often remove and substitute the illegal contents with legal look-alike substances (e.g., cocaine → potato flour) before resealing and restoring the shipment to its original appearance. Not to raise any suspicions among the recipients, the police try to adhere to standard delivery times when executing a controlled delivery. Depending on the circumstances, the police let either the regular postman or an undercover agent deliver the shipment to the suspect. "Every situation is analyzed by the senior police in charge," the Cantonal police officer stresses. "It's not black and white." He rightly reminds that the indicated shipping address of an illegal delivery might not be the address of the actual receiver. The recipients may order contraband to their home addresses with their real names, but many buyers prefer to use P.O. boxes or post restante addresses or order goods to vacant holiday houses or any other unoccupied buildings, called drop houses. Some may persuade their friends, relatives, or acquaintances to receive illegal shipments on their behalf. "Maybe the addressee has children, friends, or roommates who are the real recipients," the representative of the Cantonal police remarks. "So, having your name and address on a cocaine shipment, even if you accept the delivery, accounts for anything but conclusive evidence in court." If the crime is serious enough and evidence warrants, the police might raid the suspect's house to collect additional evidence[85]. "In case of a drug seller," he continues, "we would probably find more drugs, ready-for-sale bags, money, and papers explaining how much [has been sold], when, and to whom." P.O boxes and poste restante address allow postponed pick-ups. In such cases, the police can set an alarm, the police representative describes. "We can ask the post office inform us as soon as the [suspected] guy is coming, and we need to ensure that the nearest police station is ready to send police officers to the post office to arrest him. […] In major cases, we could place police officers inside the postal office." But anyways, the magnitude of the response depends on the seriousness of the crime and available resources. "If it's for twenty grams of cocaine or heroin, we are not going to put a police officer to a post office for days. But if we had information that two kilos [of drugs] are coming today, we would stop other activities and send most officers to this case."

[85] Judges arbitrate the case based on all available evidence including interviews, transaction records (SMS messages, e-mails, notebooks), and forensic evidence including fingerprint and results of a DNA analysis. "Even if someone pleads guilty, that's only a part of the evidence," a representative of the cantonal police says. "Someone could take the blame for a crime even if he hadn't done it." Thus, investigative efforts should generate sufficient evidence that show that the recipient has in fact ordered illegal goods, and done it deliberately and voluntarily.

The Swiss territory is divided into 26 cantons, semi-autonomous administrative districts that wield strong political influence over internal matters. Among other prerogatives, each canton runs its autonomous cantonal police forces, which are competent to deal with all criminal offenses in their respective cantonal jurisdictions. The Federal Office of Police (FEDPOL), headquartered in the Swiss capital Bern, has no power over the sovereign cantonal forces. Instead of oversighting, the federal police takes care of the international police cooperation, in particular with EUROPOL and INTERPOL, and fights terrorism and cyber crime at the federal level.

Box 11 Swiss police forces

5.3.8. Mailroom security

Some companies and government agencies have decided to screen their incoming postal traffic for security threats to protect their staff. The mailroom security controls are voluntary and based entirely on the organizations' internal safety and security policies. Technically, the mailroom security controls take place outside the postal delivery network, after the postal service has done its job by delivering mail to rightful recipients. Typical mailroom security procedures take place in separated mailrooms and employ X-ray screening. Depending on what threats are targeted, also material trace detectors and sniffer dogs may be used to complement the X-ray screening. In case biological threats are targeted, mailroom security personnel may radiate, fumigate, or heat mail items to kill biological agents such as anthrax bacteria. When threats are detected, the security personnel may call a police bomb squad to take care of bombs or firefighters to deal with biological, chemical, or radiological threats.

Not all organizations, that seek extra protection, carry out mailroom security themselves. For extra security, a group of security-concerned organizations sometimes purchase the outsourced service even if they have mailroom procedures up and operational at their own premises. To response to demand for security services, Swiss Post has set up mail screening service for clients who prefer to outsource the mailroom security. The Swiss Post's mailroom supplementary security service involves X-ray screening for explosives in a separate Swiss Post-operated screening facility. This service, according the Swiss Post manager, adds one day to the regular delivery time.

5.3.9. Inadvertent discovery

Sometimes illegal and/or dangerous contents of postal items get disclosed during regular mail handling procedures. It should be remembered that Swiss Post opens postal items in the Swiss postal system only on warranted suspicion, when postal employees suspect that an item could harm themselves, their colleagues, or recipients. Otherwise, under the Swiss law on the secrecy of correspondence, Swiss Post's employees are not allowed to open postal items, let alone

examine their contents. Exceptions to this rule are Swiss Post's customs brokers who operate under the Swiss customs' mandate and who can thus open imported and exported postal items without violating the law.

The first opportunity for discovering contraband is when customers hand over their items at post office counters. At this point, the post office clerks routinely assess whether postal items are too fragile or bulky for the postal delivery. The clerks have also opportunity to ask questions about the contents, observe the sender's behavior, and examine the items for suspicious features such as oil stains, obtruding wires, or ticking noise. If the clerks' suspicious arise, they may refuse to accept the items and even call the police. However, there are certain critical limitations to the pre-acceptance screening. First, the pre-acceptance screening is only a superficial check by four human senses: sight (appearance of packaging), touch (weight & texture), hearing (ticking noise), and smell (strange odors). Moreover, the cursory screening applies only to over-the-counter mail: postmen collect letters from public mailboxes in postbags, so unlike the post office workers, they do not handle mail items separately. Finally and most importantly, post office personnel are not trained, obliged, nor equipped to search possible contraband or security threats. "We have limited means to prevent forbidden goods from entering the postal system," the Swiss Post's security manager concludes. "When somebody comes to a post office counter, he can pretend everything. You cannot know whether the contents match the product description. […] If the sender declares something illegal as books, we ship the item as if books were inside."

Illegal contents may also get exposed when parcels and envelopes get accidentally broken in the regular mail handling process. "When a parcel breaks and something suspicious comes out – liquid, powder or something potentially dangerous or illegal – we need to react," the Swiss Post's manager explains. "For example, if we suspect drugs, we call the police." Postmen, sorting staff, and other people handling the postal items are instructed to notify their superiors, security personnel, or authorities if they encounter anything suspicious. But again, the postal personnel are rarely able to distinguish potato flour from cocaine, doping substances from legitimate mail-order medicines, or a fake Louis Vuitton dress from a bona fide piece of haute couture. In case of the counterfeits, the distinction between a fake and a genuine product is challenging even for professionals who have the right tools and know-how. Many times, counterfeits are crafted by skilled artisans from authentic materials in a way that matches the quality of genuine products.

The counter-screening and the accidental breaking are exceptional, inadvertent ways for Swiss Post and Swiss law enforcement authorities to get know that illegal goods are inside postal items. By far, most illegal goods are detected during the import clearance process when Swiss Post's customs brokers declare postal traffic item-by-item to the customs. The brokers are personally responsible for the declared data, so they must open the postal items and verify their

contents whenever the information the sender provides in CN22 / CN23 customs forms appears inadequate or suspicious. If upon opening the brokers encounter anything illegal or dangerous, they are obliged to notify their superiors and/or people at the customs. Table 32 summarizes the three main mechanisms through which illegal or dangerous contents of a postal item may be exposed to the Swiss Post and the Swiss authorities as part of regular mail handling process, outside any particular postal security control domain.

	Observers	Description	Precursors for discovery
Pre-acceptance screening	Post office workers	General alertness for suspicious items and senders.	Suspicious features / behavior
Accidental opening	Mail handlers	Items may get accidentally broken in the handling process.	Fragile packaging / rough handling
Preparation of import declaration	Customs brokers	Postal items might be opened in the import clearance process.	Incomplete / illegible / suspicious information

Table 32 Ways of inadvertent contraband discovery

5.3.10. Anti-theft measures

Swiss Post is naturally concerned of the anti-theft security throughout the international postal delivery network. A look on theft statistics reveal that mail theft rates have been very low in Switzerland constantly, which suggests that Swiss Post's organization is already fighting mail theft rather effectively. Nevertheless, given the zero-tolerance policy for mail theft, that Swiss Post pursues, there is still potential for further improvement. Particularly, new mail order services (e.g., online currency exchange service or coffee capsule refill scheme) call for advanced anti-theft security solutions. Also, Swiss Post and other postal operators, thanks to the expanding e-commerce traffic, are today carrying increasingly cameras, tablet computers, cameras, and other theft-prone high-value electronics.

Physical security measures – fences, burglar-resistant doors, locks, and so forth – play a key role in securing the postal service from unauthorized people. Beyond the four walls of postal logistics facilities, protection of postal items from thieves gets harder. External thieves often hit at the final delivery stage, and they steal from unattended pick-up and delivery vehicles as well as private mailboxes. "Postmen sometimes leave their cars, mopeds, or bicycles unattended when they bring the post inside the house," the Swiss Post's representative describes the behavior that exposes mail to theft during delivery rounds. To reduce the exposure, Swiss Post has instructed their postmen to follow security procedures, most notably lock their vehicles and keep an eye on mail pieces. Besides preventing unauthorized people from getting their hands

on mail, Swiss Post is committed to fight internal theft. "In most cases, items are stolen by employees of the post in the sorting centers or by postmen," the Swiss Post's manager points out. Some postal employees may be tempted to steal mail because they have legitimate and easy access to postal items and they have often developed an eye for identifying worth-to-steal postal items.

Sometimes mail gets stolen no matter how strong anti-theft protections are. In such unfortunate cases, mail theft investigations typically start when a recipient or a sender finds out that her mail piece has not arrived. "We can really solve only repeating cases – when you have thefts always at the same place," the Swiss Post's security manager explains difficulties in solving isolated theft incidents. "Once a postman forgot to lock the door of his van, and when he came back, something had been stolen. What can you do in that case? You don't have cameras or eyewitnesses. You cannot really expect that we would catch the thief." But when a pattern of seemingly connected theft incidents is detected, Swiss Post's own detectives set traps to catch the thieves red handed. They might send "letters that are treated with product that leave marks in the fingers," the manager points out. Swiss Post's internal detectives are mostly preoccupied with mail theft prevention and investigation. But many times, especially in serious mail theft cases, the Swiss police get involved in the investigations.

5.3.11. Mapping domains onto baseline postal logistics process

Earlier sections described the phases of the baseline postal logistics process and the domains of postal security. In this concluding section, we map the security domains onto the baseline end-to-end postal delivery process.

Letters and parcels brought to post office counter may get visually screened. This entry screening, however, is a cursory check post office clerks do to prevent fragile and bulky items from entering the postal system. The check is not about ascertaining whether the items contain contraband or security threats. The first actual contraband and security screening may take place later when foreign-bound postal items are about to leave Switzerland. The exported postal items are sometimes inspected by customs and other border control agencies. The border controllers determine the need for and type of inspections by comparing traffic information against risk profiles that indicate high risks. This risk assessment exercise uses consignment-level exit notifications and item-level export declarations as the input. Although the risk assessment is systematic, the export border controls are rare and exceptional in Switzerland. This is opposite to airmail security and safety controls to which almost all airmail items are subjected before they are loaded aboard an aircraft. Figure 21 below illustrates this outbound logistics process and associated security procedures from the Swiss perspective.

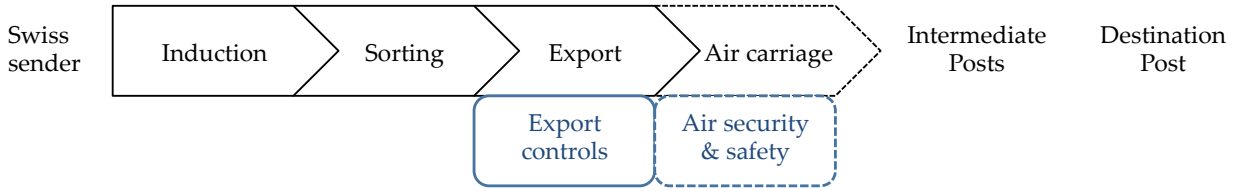


Figure 21 Postal logistics process and associated security domains for Swiss exports

Each of the 192 UPU members must exchange mail with one another, either directly or through intermediate, transit postal operators. In case of an indirect exchange, transit border controls may take place whereby customs and other border control authorities examine the transiting traffic for contraband or security threats. It seems that transit border controls are even less common than the export border controls. In fact, the authorities control transit traffic typically only when they have tactical intelligence that gives them reason to assume that illegal goods or security threats are about to traverse their territory. Sometimes transiting or transferring[86] airmail gets rescreened for airmail security and safety threats at transshipment points, sometimes multiple times before the airmail reaches its destination. Figure 22 shows transit / transfer postal handling activities and associated security and customs controls.

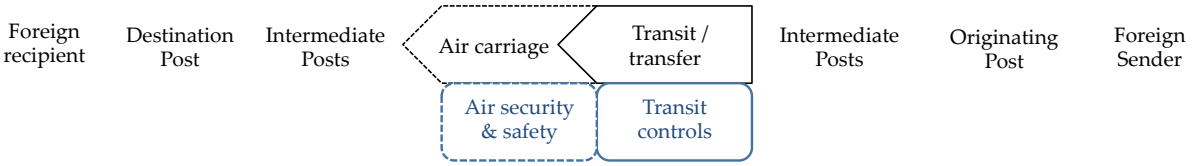


Figure 22 Postal transit / transfer process and associated security domains

Before entering the Swiss national postal system, almost all imported postal items undergo a formal import clearance procedure (recall that some items are eligible to a simplified clearance). We found that the import clearance involves three distinct security domains. The first one is the pre-declaration border control in which customs and other Swiss border control agencies target contraband and security threats that are illegal no matter what Swiss Post's customs brokers eventually declare to the customs (e.g., heroin, bombs, or counterfeits). The interviewees anyhow pointed out that the pre-declaration controls on the postal traffic are currently relatively rare. The second security domain is the parcel bomb screening that Swiss Post, ever since a parcel bomb exploded in Olten in March 2011, has been conducting voluntarily on all surface parcels that need to be opened in the customs clearance process. The third security activity is the post-declaration control during which customs officers have an opportunity to verify whether the declared contents of a postal item corresponds to its actual contents. Physical

[86] Recall that the difference between transit and transfer airmail is that transferring traffic is moved from an aircraft to another while transiting traffic stays aboard the same plane.

examinations of the contents and shipping documents are relatively common at this stage. After the mail items clear customs and enter the Swiss postal system, they rarely ever encounter controls. As an exception to this rule, mail addressed to some organizations might undergo security screening in the mailroom of the addressee. Moreover, police authorities may intervene with the postal traffic in exceptional occasions. The police operations are not systematic, but rather based on actionable intelligence or exceptional security needs (e.g., a bomb threat). The police authorities collectively can intervene with the postal traffic virtually anywhere in the international postal network. Figure 23 summarizes the import process and associated security controls.

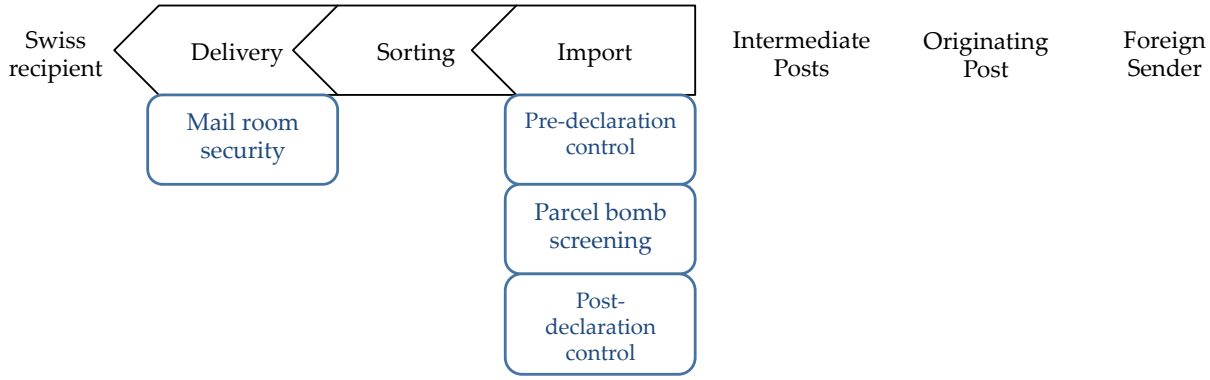


Figure 23 Postal logistics process and associated security domains for Swiss imports

Anti-theft controls and police operations are security activities that cannot be pinpointed to a specific location in the international postal delivery network. In case of the anti-theft controls, the whole network is somewhat protected from unauthorized people with locks, camera systems, alarms, and other physical security and surveillance solutions, though some sections are certainly better protected than others.

Interestingly, we found that the domestic Swiss postal traffic gets almost never controlled for any type of contraband or security threat. The reason for the apparent absence of controls in the domestic traffic seems to be threefold. First, by definition, the domestic traffic is not subject to import, transit, or export border controls. Second, because of relatively short distances inside Switzerland, few domestic mail items take airplane and therefore undergo aviation security and safety controls. The third reason for the seemingly lax controls in the domestic traffic is that the only control domains that actually concern the domestic mail flows – police operations and the mailroom – become active only under special circumstances when there is evidence to believe that crime or terrorism has occurred or is about to occur in the postal system.

What is more, the security controls appear relatively lenient also in case of the international traffic. Border controls for departing and transiting postal traffic are rare and often triggered in exceptional cases only when actionable tactical information is indicating immediate security

risk. Import border controls are the most stringent control domain in the overall postal network. Even so, roughly one percent of the imported postal items get physically examined by the customs officers or other Swiss border control agencies in the post-declaration controls. Against this observation, the border controls do not seem very stringent after all. But the border controls are rather lenient, airmail security and safety controls appear strict. According to the EU's aviation security regulations, every single airmail item must be screened before it is loaded onboard an aircraft. Extra intense screening might be applied to high-risk cargo and mail (HRCM) items. All this security is reasonable to assure adequate aviation security. However, the rescreening of airmail shipment at one or more transshipment locations seems a redundant waste of limited security resources.

Only explosive and incendiary devices, that are threats to airmail security, are systematically screened in the postal traffic. Also imported surface parcels, which must be opened in the customs clearance process, are screened for explosives to protect Swiss Post's customs brokers and their colleagues at customs. Sometimes receivers themselves screen postal traffic as part of their internal mailroom security programs. The key observation here is that the airmail, the to-be-opened surface parcels, and items going through the mailroom security account only a small part of the total international postal traffic. Meanwhile, for the most part, the rest of the traffic is left without any screening for explosive, biological, chemical, or radioactive weapons – the security threats. Granted that also outside the airmail domain, the postal items face may face export, transit, import border controls. But after all, the likelihood of facing the inspection is small. This means further that the international postal traffic in general is only sometimes checked for explosives and rarely for other security threats and many types of contraband. Table 33 summarizes the security control areas of the postal logistics network, informs what segments of the postal traffic they cover, what types of threats they target, and how common the controls are.

It should be noted that there are evidently secret security and customs controls in place in the postal logistics network, which complement the overt controls described in the pages to follow. "We have invisible measures of which only security specialists are aware," the security manager of Swiss Post remarks. "[…] It would be unreasonable to disclose all our security measures to the public." Also the Swiss authorities apparently keep certain security solutions secret. Civil aviation authorities, for instance, maintain confidential aviation security programmes, which specify detailed techniques and focus areas of airmail security procedures. Likewise, customs authorities in Switzerland and elsewhere do not often disclose high-risk indicators and profiles they use to risk assess traffic and select shipments to border controls.

Control area	Coverage	Targeted threat / contraband	Commonness of intervention
Export border controls	All traffic	Absolute & relative	"Rare" "Exceptional"
Aviation security and safety controls	Airmail	Security (explosives) & safety	One-hundred-percent
→	Open transfers Closed transfers if air carrier requests	"	"
Transit border controls	Transits	Security, absolute & relative	"Very rare"
→	"	"	"
Pre-declaration import border controls	All	Security & absolute	"Maybe a few times a year" except for periodic high-intensity campaigns
Supplementary security	Surface parcel imports if opened in the clearance process (≈ 30 % of all parcel traffic)		One-hundred-percent
Post-declaration import border controls	All traffic	Fiscal & relative	≈ 20% blocked, ≈ 1% examined
Police intervention	All traffic	Absolute	"Very rare"
	Mail to suspects	N/A	One-hundred-percent
Mail room security	Mail to exposed organizations and individuals	Security	Depends on organizations' internal policies
Anti-theft controls	All	N/A	Varies from location to location

Table 33 Postal security domains by traffic type, targeted contraband and frequency of intervention

Summary

This case study chapter described the international postal service from the Swiss perspective, putting a special emphasis on postal security management and law enforcement. The case study evidence revealed that there are nine main domains of postal security management, each aiming at their distinctive goals and employing a different set of security solutions. Closer scrutiny of these security domains revealed that security activities differ markedly across different types of postal traffic and in terms of what crime types they address. The airmail traffic was fond far the most secured segment of the international postal traffic, owing to the relatively stringent aviation security regulations that impose, few exceptions aside, 100% screening on all airmail items. We found, however, that the airmail security screening targets explosive and incendiary devices. Other types of security threats (biological, chemical, and radioactive) and contraband in general might get controlled in border controls when the postal traffic cross frontiers. The border controls are anyhow rather lenient, as only a small percentage of postal traffic is physically inspected. Finally, once the postal items pass border controls and enter the Swiss postal system, they are no longer subject to any controls, expect for occasional yet rare police operations and mailroom security procedures.

Chapter 6 | Case study analysis

This analysis chapter seeks to identify evidence-based concepts for improving the postal security management by taking a theory-based view on the contemporary challenges of the Swiss-centric international postal service. The analysis applies the design principles of logistics-friendly supply chain security management as the theoretical basis (Ch. 3) and the case study evidence as the empirical bedrock (Ch. 5). The chapter concludes by summing up key findings and recommendations to the postal security management in Switzerland, in the European Union, and worldwide at the Universal Postal Union level. The analysis and resultant recommendations are loosely categorized under the five themes of the model of logistics-friendly SCS management. It should be noted, however, that many of the improvement concepts this chapter present are influenced by more than one design theme.

6.1. Mix of solutions

The literature synthesis showed that it is not indifferent what security solutions are selected and how they arranged: some security solutions are complementary and bring synergies, sequence of the security solutions matter a great, and so do alarm thresholds. This section discusses what factors decisions makers should consider when they select and implement security solutions in the postal logistics context.

6.1.1. Scope and selection logic of intensive airmail security screening

Soon after the Yemen bomb plot in late 2010, the European Commission issued a new regulation (859/2011) that defined common criteria for identifying and screening of high-risk cargo and mail (HRCM). The novel HRCM regulation introduced a rule-based approach for determining which shipments require intense HRCM screening. The rules stated that all shipments that have signs of tampering, are flagged suspicious by tactical intelligence, or come from or transit through high-risk countries are to be screened up to the intense HRCM screening standards. Today, a few years later, the Commission's new Union Customs Code is about to extend the advance electronic information (AEI) requirement to cover certain segments of the postal traffic and to introduce an early deadline for lodging the AEI data set so that EU customs can risk assess airmail items before they are loaded onboard an aircraft. As part of the

customs code reform[87], the Commission is moving from the rule-based approach to a score-based approach. Under the envisioned score-based approach would no longer be determined only based on the static risk-rules but also based on dynamic item-level risk analysis. The analysis would compare risk levels of individual shipments case-by-case by assessing item-level data against a set of predetermined high-risk indicators and risk profiles. The more severe high-risk indicators a shipment meets, the higher its risk score grows, and the more likely the item is selected to the HRCM screening.

Postal items may lose time in the intense high-risk cargo and mail screening and associated supportive logistics tasks such locating the receptacle containing the targeted item; unloading of item from the receptacle; moving the item from staging are to the HRCM screening facility; queuing up for HRCM screening; passing the HRCM screening; moving back to the staging area; putting the item inside the receptacle; and resealing the receptacle. Due to the time lost in the piece-level HRCM activities, the postal items may miss their flights and fall behind their delivery schedule. Moreover, due to the extended processing time and the extended processing time variability, Posts should bring outbound airmail to the exchange office hours before the scheduled flight takes off. It is important to note that the delay, though justified on grounds of aviation security, is detrimental to customers satisfaction: senders and receivers perceive no difference between delays that stem from HRCM screening and delays that occur due to some less excusable reason, such as sloppy management. Therefore, it might a good idea to remind the customs that the HRCM screening is subject to process and capacity constraints, and if these constraints are not respected, airmail traffic is slowed down and customer satisfaction is likely to fall. Authorities might be able to reduce delays related to the HRMC-screening because, in principle, they could influence the rate of HRCM screening by adjusting sensitivity of their risk assessment algorithms.

It is crucial for the both rule-based and the score-based risk assessment approach that they are based on rules that are meaningful from security perspective and practical to implement from the postal logistics perspective. It was officials of the US Transportation Security Administration who introduce an impractical security rule to airmail traffic in the immediate aftermaths of the Yemen bomb plot. The rule obliged postal operators worldwide to screen heavier than 453g (16 ounces) US-bound airmail items at piece level up to "top security" standards, if the items were to be carried on passenger planes. Besides the stringent piece-by-piece screening, a "tendering statement," a pledge that item originates from an established business partner, was required for each item exceeding the weight threshold. From the security perspective, the rule made sense

[87] Remember that the European Commission is preparing the Union Customs Code (UCC) that is to be replace the old Community Customs Code (and recast, i.e., amend the Modernized Customs Code). The requirements of the UCC are projected become applicable stepwise between 2016 and 2020.

because items from unknown senders clearly pose higher risk than items from trusted business partners, let say established online retailers or government agencies. But although the rule made security-sense, it seriously handicapped the US-centric international airmail logistics for weeks because the postal operators were unable to comply with the rules efficiently: the Posts had hard time collecting the tendering statements (after all, Posts do not have "established" relation with private senders) and segregating the few items with the tendering statement from the bulk of the postal traffic.

In the EU, the new Union Customs Code legislation should also define the range of threats addressed, in particular should the pre-loading risk assessment target on IEDs that endanger aviation security and the later pre-arrival data to target also general security risks or certain types of contraband. If the regulation is to address aviation security risks only, the referral options should be limited to screening to HRCM standards and Do Not Load messages. The narrower scope of the threats would also reduce the need for HRCM screening.

6.2. Capacity & intensity

The literature synthesis suggested that capacity and intensity of security solutions affects drastically logistics and security performance. The next sections elaborate how Swiss Post and Swiss authorities could improve their approaches to postal security management to become more able to cope with security-induced uncertainty.

6.2.1. Adaptive and responsive control systems

The case study evidence suggests that, except for airmail, only a small percentage of the international traffic gets inspected for *any* contraband or security threat. However, a Cantonal Police as wella as representatives of Swiss customs, and Swiss Post emphasize in unison that the present controls are proportional to the current level of crime and terrorist threat in Switzerland. The representatives also assured that they could step up security controls if changes in the overall threat landscape prompted them to do so. "We would increase security level and get ready," the representative of the Cantonal Police guarantees. "We have different levels of security that correspond to the present terrorist threat." He explains that the cantonal police are vigilant for all criminal threats all the time, but under normal conditions, the day-to-day policing is preoccupied with mundane crime problems. "We could have anthrax once for real. After that, it [preventive action] is a question of proportionality. Do we employ hundred officers to enforce something twenty-four-seven? Depending on the seriousness of the offense, we will invest more time." Like the cantonal police, Swiss customs monitors closely criminal and terrorist trends. "We fix our priorities based on threat scenarios," a risk management expert from Swiss customs clarifies reasons for concentrating customs controls on certain types of goods, modes of transport, trade routes, and types of traders. He adds that Swiss customs has

mobile inspection teams at hand that can be dispatched immediately to control urgent threats. Similar to the law enforcement authorities, Swiss Post can adapt its operations for higher security; the company maintains unused screening capacity, has access to extra guarding services, and fosters close relationships with fire brigade, the police, and other "blue light" emergency authorities. But again, as long as there are no sign about new security threats, Swiss Post continues to do business as usual. "All the time, our security measures are always based on risk analysis – frequency times consequences," a Swiss Post's security manager says.

The key stakeholders say that they are prepared to deal with security emergencies if they should occur. But beyond the reassuring rhetoric, what does preparedness mean in the postal logistics context in practice? One day, for the first time in history, we might discover anthrax or other lethal biological weapons in the European postal system, even in Switzerland. Being prepared for the weaponized anthrax would mean that the authorities (or postal operators) would be able to rapidly deploy fumigation, heating, radiation, and other neutralization techniques for eliminating the anthrax bacteria. In few days, they should have secured the most exposed customers, vulnerable critical postal facilities, and risky traffic flows. Later, especially if the anthrax threat escalates further, the authorities should be able to roll out protection across the whole European postal system, in post offices, sorting centers, and other sites where no screening currently exists. Such a large-scale and urgent anthrax protection program would require solid emergency plans and some preliminary investment in anthrax screening systems and expertise. Ideally, existing sorting machines would have a modular design so that anthrax detection / elimination instruments could be easily mounted on the present sorting systems for cost-efficient screening.

Early information about emerging threats gives time for the authorities and the postal operators to get prepared to respond to the imminent threats. To get timely information, Swiss customs' officers in Bern, at the Situation and Information Centre, exchange information (e.g., seizure statistics, exemplar X-ray images demonstrating concealment techniques, and movements of suspicious cargo and people) with their EU colleagues. The EU-level information exchange has been more intense since the Agreement on Customs Security and Facilitation entered into force in 2011. The agreement established principles for sharing law enforcement sensitive information on high-risk indicators and profiles as well as results of risk assessment among the customs administrations across the EU customs security area. At the global level, Swiss customs shares and gets information through the WCO's Customs Enforcement Network (CEN). Main domestic sources of law enforcement intelligence include the cantonal and federal police forces, and the Swiss Federal Intelligence Service (FIS). The Swiss police forces exchange law enforcement intelligence nationally, and with foreign police forces mainly through INTERPOL, a trusted messenger between police authorities worldwide. Besides relaying the law enforcement information between its members, INTERPOL produces many intelligence

products on its own, especially in form of color-coded crime alerts, called notices. The purple alert is particularly useful for anti-smuggling law enforcement as it warns about changes in criminal "modi operandi, objects, devices, and concealment methods."

It is crucial that the authorities and the postal operators acknowledge the importance of capability to cope with new threats and monitoring of risk landscape, two key concepts for dealing with the security-induced uncertainty. Even though the current postal security situation is stable and void of serious threats, this period of tranquility can break at any moment. "It's a matter of time when the next incident happen. The question is only when and how," as a Zurich-based air cargo security specialist puts it. Incidents involving mail bombs, anthrax, chemical substances, or even more exotic threats we have never thought of, may occur, and if they should, fast and effective response is crucial for protecting the public and restoring its confidence to the postal service. We are unable to foresee all threats, so the authorities and the Posts should monitor the threat landscape relentlessly, create emergency plans, and build security expertise proactively. They should make some preliminary investments in modular screening solutions that could be adjusted to address new threats, and that could be scaled up to meet higher screening intensity and/or increased traffic. Border control authorities should consider setting up more mobile inspection teams that would be used to deal with local congestions or to execute focused law enforcement campaigns.

6.3. Secrecy of information

The literature synthesis concluded that secrecy of security information sometimes improve and sometimes reduces effectiveness of security systems and logistics operations. Therefore, any security information should always be disclosed sparingly, aware of advantages and disadvantages. The following sections discuss how to strike a balance between secrecy and openness of security information in the postal logistics context.

6.3.1. Indicators of security sensitivity

In the airmail security domain, the practice of clearly indicating security-sensitive items is the law: secured, identifiable airmail must be kept separate from surface mail, and secured airmail must be kept separate from unsecured airmail. This practice works because all employees, who can access the identifiable airmail, have gone through background vetting and can be thus in principle considered as trusted personnel. These employees also work under managerial supervision in high security facilities such as at airport airmail exchange offices. Hence, although the employees can identify security-sensitive airmail, given their checked trustworthiness and their secure working environment, they are unlikely to tamper with the identifiable airmail and insert explosives inside. But the situation is different outside the airmail domain where backgrounds of staff members are not necessarily vetted, and where workers

may spend long time with mail items without supervision. Under these circumstances, we may ask whether it is reasonable to indicate theft-prone insured items with pink CN 06 labels like some UPU members are doing. Or whether it is wise to carry insured letters in distinctive red satchels like one Nordic postal operator used to do a few years back.

In general, indicators of security status or high value make it easy for postal employees to keep an eye on the theft-prone items and handle them with extra care. But, at the same time, these indicators help potential thieves find valuable items that would have otherwise remained unnoticed underneath piles of less valuable postal items. Overt anti-theft features often have the same effect than the distinctive markings. Security tapings, for instance, helps detect and investigate theft as the taping makes it harder for thieves to open envelopes without leaving obvious marks of tampering. But on the other hand, the security taping is a flagrant clue that indicates that the postal item contains something valuable, for the very reasons that the sender is making extra effort to security the item. Parcels and letters sometimes display brand names, logos, and return addresses that indicate what is inside. These markings are also valuable clues for potential criminals who are looking for items to steal (e.g., electronics, cash, concert tickets) among thousands of postal items, most of which are not worth of stealing (e.g., bills, personal correspondence, books in foreign language, or marketing material). Because it is better if the thieves do not know whether a standard package contains consumer electronics or something less interesting, a good way to reduce theft would be hide valuable targets by removing distinctive markings from external packaging. The hiding of indicators of high value proved an effective solution to fight theft of cash envelopes that some Swiss banks mailed as part of their online currency exchange service. A few years ago, Swiss Post observed that exceptionally high percentage the currency envelopes got lost in a certain delivery area. When the banks followed Swiss Post's guidance to start posting the cash in standard manila envelopes with hand-written addresses, the rate of lost deliveries fell. The most likely explanation for the lower loss rate is that he thieves could no longer distinguish cash deliveries from the bulk of the ordinary mail.

In the international traffic, we cannot always remove all indicators of high value because of customs controls. In particular, most international postal items travel with customs declaration forms (CN 22 and CN 23), which reveal type and value of the contents, therefore helping potential thieves – dishonest postal workers, corrupt customs officers, or external pilferers – to identify attractive items to steal. This is why, anecdotal evidence suggests, some watch owners declare false information in the CN22 and CN23 customs forms: they want to hide the contents from the potential thieves. In the future, instead of resorting to this insincere technique, we could hide the content information by converting the written customs declaration information into a digital format that would be illegible to the naked eye. This way, in principle, only trusted customs brokers and officers, who would be equipped with optical readers, would get access to the content data. Another good way to keep postal items away from the potential

thieves is to carry them in sealed, opaque mail aggregates, such as bags, covered trays, and other receptacles, whenever possible. Stealing an entire receptacle makes little sense because most items inside would be most likely worthless for the thief and because theft of multiple items would be more likely detected and investigated than pilferage of a few single items over time. Closing the receptacles with tamper-evident seals would also help detect unauthorized tampering and speed up the start of investigations.

6.3.2. Communication of security principles

Secrecy of security information can also be counterproductive both from the security and logistics perspectives. In the air cargo and mail screening, higher security and operational efficiencies may remain blocked because the authorities do not share detailed enough threat information with the industry. "Instead of telling what to look for, they tell us operators just to look harder," a cargo security expert points out at the IATA air cargo and mail security conference in 2013. Another expert complains that authorities sometimes share the threat information with the operative screening staff but not with their superiors, thereby making managerial supervision more difficult. Moreover, if information does not flow freely between concerned parties due to confidentiality, emergency responses might get slowed down.

As the literature synthesis suggests it is often reasonable to make people aware of the presence of covert security solutions, boast the effectiveness of these hidden solutions, but not describe in detail how these solutions function. This approach increases the deterrence effect without giving away any information that would help potential criminals to circumvent the security solutions. Consider, for example GPS-based tracking devices, which are able send real-time information on the status and the location of a postal item. If the tracked item got lost, the tracking information would allow investigators to ascertain the location and the time of the loss and go after those people who most likely have had something to do with the lost item. Interestingly, if dishonest staff members knew that some postal items are mounted with the GPS trackers, they would understand that if they stole a tracked item, they would very likely get in troubles. However, as the staff members had no clue which items contain trackers, they would think that the risk of stealing *any* postal item would have increased and as a result, they would be less willing to steal. Therefore, to intensify the deterrence effect, people should be made aware of the possibility of random or secret security measures and their effectiveness.

6.3.3. Degree of randomness in security controls

Introducing randomness into security controls may intensify further the desirable deterrence effect. At sorting centers, mail theft could be reduced if employees faced a risk of getting inspected at the end of the day as they exit the facility. The possibility of facing the inspections

at the exits would discourage theft, quite the same way than the risk of facing a billet controller deters commuters from using public transportation without tickets. In the anti-smuggling postal security, customs commonly make use of a degree of randomness when they control cross-border postal traffic. Owing to the randomness of the controls, every single postal shipment might get inspected in a spot check, regardless of its risk score given by the automatic risk assessment system. The idea of this randomness is to make sure that there are no foolproof techniques for avoiding border controls altogether, and thus criminals can never be certain that they get away with their crime. Also changing control priorities, screening methods, patrolling rounds, and other security procedures make criminals less able to learn and exploit weaknesses of security systems. The changes also keep the employees alert and vigilant.

6.3.4. Reduction of anonymity

Senders and receivers of contraband shipments take their anonymity seriously, as long as debates at the Silk Road forum, an infamous online black market, stand for sufficient evidence. Also past mail bombing investigations have revealed that terrorists, even those claiming attacks publicly, have often disliked the idea of being traced down and raided by the law enforcement. The smugglers and the terrorists alike appreciate the shroud of anonymity the postal service offers. Hence, lowering anonymity seems a feasible way to make the postal service a less preferable channel for sending illegal items or security threats. Currently, mail provides strong anonymity to the senders who can mask their identify simply by writing a wrong return address and dropping their items into a public mailbox. The recipients need to make more effort to disguise their identity because mail must be addressed to somebody. Swiss Post could ban cash payments and require IDs upon sending a postal item only in exceptional cases, when the item is destined to a high-risk region or a vulnerable recipient (e.g., a prominent politician). I also recommend Posts, which still offer pseudonymous poste restante addresses or P.O boxes, to stop providing such services because the pseudonymous addresses get in some cases abused by buyers of illegal online merchandise. Alas, the reduced anonymity would come at a cost of the discretion and convenience of the postal service. However, a handful of privacy aficionados aside, law-abiding citizens lack rational reasons for sending postal anonymously to anonymous addresses. The convenience is therefore a bigger problem than the privacy, at least in my personal view. Swiss Post could lower the senders' anonymity by banning cash payments and requiring the senders to present their IDs when they hand over items at the post office counter. But such practices would make the postal service less convenient for use. The ban on cash payment would also exclude some customers segments from using the postal service (e.g., underage and elderly people not having credit cards), thus violating UPU's principle of offering basic postal services for everybody. Moreover, if the ID requirement were extended to the letter post, people could no longer drop their international envelopes into public mailboxes.

6.4. Logistics integration

The synthesis of the literature found that the way security activities are integrated into the sequence of baseline logistics activities is consequential to speed, reliability, and security of logistics processes. This section elaborates how we could integrate postal security solutions into the cross-border postal logistics network with least possible disruptions to the day-to-day, routine postal logistics operations.

6.4.1. Compliance with advance electronic information (AEI) requirement

The EU's new Union Customs Code (UCC) is going to extend the advance electronic information (AEI) requirement to the postal traffic. Due to this regulatory reform, postal operators must start sending item-level entry and exit summary declarations to EU customs around 2016 – 2020, when the legal requirements of the UCC become applicable. Not surprisingly, there are many unsettled questions regarding the new advance electronic information (AEI) legislation.

The first question relates to the timely and cost-efficient capture of item-level AEI data from exported postal items. We learned earlier that letter post items enter the postal system through a variety of access points, including public mailboxes, unmanned parcel drop terminals, post offices, and third party operated post offices. It was apparent that currently, only international parcels and registered letters travel with unique item-specific bar code identifiers, and without the item-level identifiers, it is impossible to connect the digital AEI information to physical items. This issue calls for extension of the tracking & tracing to all postal item categories that fall within the scope of the new AEI legislation. We also found that senders sometimes provide no information when they send small international letter-post items. Also when they provide the information, it is not digital but written in CN22 and CN23 forms. The diversity and the large number of access points make electronic capture of CN22 and CN23 information, that is most likely to be the AEI dataset for the postal items, challenging. Tailored solutions should be designed for each distinctive access points. The operation logic of the unmanned parcel terminals might need to be changed so that relevant information gets collected upon sending. At the post office counters, one way to capture the item-level AEI information is to bring self-service computers to the post offices that allow the senders to fill out the necessary shipping information electronically. The customers could also prepare their shipments online, and provide all consignment details over the web. But inevitably, at the moment, the only way to capture the data for some product categories, let say items dropped in public mailboxes, is to capture hand-written information manually at the post office counter or later in the postal logistics network, for instance at the first sorting center or as late as at the airmail exchange office. The delayed manual data capture is the least preferable alternative for collecting the AEI

data due to its costliness and associated delays. Box 12 offers some insight to whether Posts could introduce a security surcharge to cover some costs of the manual AEI data capture.

Manual transfer of the Entry Summary Declaration AEI dataset from the paper-based CN forms to a computer systems takes time and implies extra labor cost. Before the new Union Customs Code becomes applicable, Posts must consider ways to cover costs of the electronic data capture. Perhaps Posts could introduce a security surcharge? Many express couriers, including TNT Swiss Post, are already charging security surcharges for express shipment to "partially offset" the cost of the post-Yemen airmail security requirements. However, unlike the private express couriers, Posts lack freedom to factor the cost of the extra security into the postage fee due to the price-sensitive low-cost market segment most Posts are operating in, and due to the government-regulated postage fees. The security surcharge would definitely hurt the e-commerce, especially the low-cost market segment where many Posts have strong footholds. An average online mail-order purchase costs around 50€, and e-shoppers are generally unwilling to spend more than one-third of the product price for shipping fees (IPC 2010). No doubt, few people would order a ten-dollar-item online if a security surcharge inflated the shipping beyond fifty dollars. Anyhow, a modest surcharge would not technically violate the EU's Postal Directive that states tariffs of universal postal services should be affordable, cost-oriented, transparent, and non-discriminatory (97/67 Art. 12). Even so, Posts should be looking for alternative ways to offset the cost of data capture. They could, for example, promise a day-certain guaranteed delivery if clients provided electronic data.

Box 12 Can Posts introduce a security surcharge to cover costs of AEI data capture?

Poor data quality is likely going to be another challenge of the AEI dataset. This challenge particularly releveant for the private customers who, unlike the business clients, are often unaware of customs formalities and might thus have problems providing information like "detailed description of goods" or "HS tariff number[88]." It is also way easier to capture the electronic data from big commercial mailers than from smaller enterprises or the private customers. Amazon.com, a global e-retailer giant, for example, already shares electronic shipping data with its carriers and uses barcoded shipping documents to ease the electronic data capture. Altogether, the optimal data capturing solutions depend largely on the postal operator's retail network (e.g., share of outsourced post offices, called "agencies"). In Switzerland, where almost everyone can access the internet, the optimum would be to educate the customers to use online interfaces for lodging the CN23 data (=AEI dataset) prior sending the postal items. But this requires, as a security expert of the French la Poste summarizes, "a huge 'customer education program' to get customers to provide adequate information and a 'digital conversion program' to get most senders to prepare their shipment online." The task of

[88] The HS system (Harmonized Commodity Description and Coding System) is a standardized international nomenclature for classifying traded commodities. The system is developed and maintained by the World Customs Organization (WCO).

educating the private customers to provide accurate AEI data electronically[89] is massive in the light of statistics of **Table 34** suggest: in 2012, in Switzerland, private customers sent 23 million postal items abroad, an overwhelming number that anyhow accounted only for 24% of total postal exports from Switzerland.

	Export		Import		Total
Sender	Letters	Parcels	Letters	Parcels	
Business	67,6 (76%)	1,0 (62,5%)	N/A	N/A	N/A
Private	21,4 (24%)	0,6 (37,5%)	N/A	N/A	N/A
Total	89,0	1,6	179,6	3,9	274,1

Table 34 Swiss Post's international postal traffic in 2012 (million items) (Source: Dieke et al. 2013)

Another key question pertains to the timely capture of the AEI data set. Postal operators insist that the AEI data set would match the data elements of the UPU's standard CN23 customs declarations and its electronic equivalent ITMATT EDI message (see Table 35 comparison of the entry summary declaration dataset against the CN23 data elements). Customs, on the other hand, would also want to have conveyance level data on the carrier, place of loading, routing, place of unloading, schedules in addition to the CN23 elements (name and address of sender, name and address of receiver, weigh and number of packages, and description of goods). Together, the CN23 data elements and the conveyance-level data, called "7+1 raw data elements," would allow the customs to conduct rudimentary risk assessment, calcute risk scores, and request appropriate security controls item-by-item. Due to the highly contingent nature of the airmail logistics, however, the conveyance-level data elements are not available until very close prior to the loading, and there might still be a need for later changes after the take-off of the first flight. This is why the draft legislation is considering a dual filing option that would allow the Posts to send the CN23 data elements prior to loading and the carrier the conveyance-level data later, after departure when the conveyance data elements are available. Moreover, it is not always trivial to capture the electronic CN23 data in the postal delivery process before the airmail exchange office. "There will still be a significant portion of the volume for which data availability will be on or close to the critical path to outbound operations," the security expert from the French La Poste points out. "Postal items may be accepted until late in the day in areas close to the outbound office of exchange, or the geography and service features may be such that time between collection / acceptance and outbound operations may be very short." If the CN23 data were captured at the outbound office of

[89] Recall that according to the current draft legislation the AEI dataset corresponds the CN23 dataset.

exchange, exit summary declaration (EXS) activities would indeed be on the critical path for the outbound operations. Manual capturing of the EXS data, EXS lodging, and waiting for customs feedback would extend time that is needed to process airmail from the office gate to the airplane's cargo hold.

ENS data set for Posts (1875/2006, Annex III, table 2)	Level of data*	CN 23 correspondence**
Consignor	X/Y	Sender's name and address
Person lodging the summary declaration	X/Y	
Consignee	X/Y	Recipient's name and address
Carrier	Z	
Country of destination	Y	
Place of loading (if cannot deduced from other information)	Y	
Place of unloading	X/Y	
Goods description	X	Designation of content Detailed description of contents
Goods item number	X	Quantity and unit of measurement of each article
Commodity code	X	Tariff number and key (for commercial items only)
Gross mass (kg)	X/Y	Gross weight of item
UN dangerous goods code (if relevant)	X	
Transport charges method of payment (if available)	X/Y	
Declaration date	Y	Date and sender's signature
Signature / authentication	Y	
Other specific circumstance indicator	Y	Comments

Table 35 Mapping ENS data set against CN23 data elements[90]

Another debate on the AEI regulation is about whether Posts should send item-level AEI data on items weighting 250 grams or more, like the European Commission has envisioned, or only for items weighting 500 grams or more, which is position of the postal industry. The benefit of the higher weight limit is its compatibility with the UPU standards that categorize the letter post items into three formats: small letters (P, < 100g), large letters or "flats" (G, < 500g) and

[90] * X = item level, Y = declaration header level, Z = consignment level

** Other CN23 data elements are: Type of Movement Certificate (EUR. 1) and number; Number of invoices (if applicable); Number of export licenses and date of issue; Recipient's telephone number; Net weight; Value of contents in CHF; Country of origin of goods; Postage costs; and Total value of goods.

bulky letters (E, < 2000g). The current postal sorting process separates the international postal items by format and class, according to the established UPU standards. Later in the sorting process, the segregated mail types are packed in receptacles (i.e., mail aggregates such as mailbags). Under the AEI rules, the Posts would need sometimes to open the airmail receptacles and search for items that customs had flagged as high-risk and to screen the risky items up to high-risk cargo and mail (HRCM) requirements at the piece level. Limiting the AEI requirement to the bulky E-format items would facilitate the airmail handling tremendously as the Posts could screen small and large letters always in receptacles.

Another hindrance might be the customs' capability to handle a surge in entry and exit summary declarations that would follow when the postal traffic finally enters the AEI scheme. The International Post Corporation (IPC) estimates that around 70 million postal items enter the EU each month. Assuming that 25% of this volume consists of G and E format letters and parcels, which would be subject to the ENS lodging requirement under the draft legislation, the customs would receive 17,5 million postal entry summary declarations per month, and 210 million entry summary declarations per year. Considering that the EU customs processed around 36 million (non-postal) entry summary declarations in 2011 (COM/2012/0793), the entry of the postal traffic into the AEI scheme would lead to staggering 580% increase in the number of ENS declarations (and corresponding increase in the exit summary declaration). The customs administrations in the EU customs security area are not necessarily ready to receive, analyze, and make sense of the millions of additional entry and exit summary declarations that begin to flood into their systems when the postal traffic enters the AEI scheme.

6.4.2. Moving security controls upstream in the postal logistics network

The literature synthesis suggested that moving location of security controls towards the upstream of the supply chain might improve both logistics and security performance (e.g., Lee and Wolfe 2003; Sheu et al. 2006). Besides the academic acclaim, there has been a great deal of practical interest in pushing the controls towards the source of the supply chain. Most notably, the US CSI and the pending 100-% shipping container screening initiative aim to move the primary security screening of US-bound containers into foreign ports. In the air cargo and mail context, the "secure supply chain" programs allow certified shippers (known / account consignors) and logistics intermediates (regulated agents) to fly cargo without screening at airports, if certain conditions are met. But most importantly, there have been recent attempts also in the postal sector to push screening from borders and airports upstream into sorting centers. In the SAFEPOST demonstration project, a multinational consortium develops and tests solutions for integrating screening machines into the sorting systems. Is the promise of the "upstream controls" just wishful thinking, or is it a real opportunity for rationalizing postal security?

There are some valid arguments that support the idea of screening postal traffic already in the sorting centers instead of borders or at airports. Virtually all postal items go through one or more sorting centers as they travel through the postal system. Lesser mail streams converge at the gates of the sorting centers, creating an opportunity for centralized high-volume screening. The high-volume screening would bring scale benefits because the screening cost would spread over millions of items, therefore decreasing the average cost per screened item.[91] The scale benefits of the high-volume screening would in turn justify substantial investments in modern (and expensive) screening equipment, which would expand throughput and detection accuracy of the screening process. Further scale benefits would arise if postal operators concentrated security expertise and training into those few central screening facilities. This is a key consideration for Swiss Post that wishes not to "invest in [security] technology and training across the country" at each of its 1850 post offices and 430 partner outlets. The cost of the countrywide security investments would be prohibitive and benefits most likely only marginal. Another benefit of the sorting center screening is that that the postal items are handled separately, piece-by-piece in the sorting process. The piece-level handling allows convenient piece-level screening, which is deemed to bring more accurate results than screening of mailbags and other mail aggregates. The early screening at the sorting center would, supposedly, eliminate the need of screening later in the postal delivery process, where the piece-level screening would necessitate laborious and time-consuming deconsolidation of the mail aggregates.

Altogether, the high-volume mass screening at the sorting center might be the most cost-efficient option to control the entire postal traffic for a variety of threats. However, there are certain technical, legal, and security problems that strongly suggest that after all, the centralized screening in the sorting centers might not be a good idea. The so-called "not in my sorting center" assertion is perhaps the most potent counter-argument to the sorting center screening. Certainly, no one wants to discover chemical, biological, radioactive, nuclear, or explosive (CBRNe) threats in the postal system. But if such an unfortunate discovery was bound to happen, Swiss Post would definitely *not* want to discover the threat in one of its sorting centers, where health of hundreds of employees and the reliability of the entire postal service are at risk. Both false and real alarms would cause problems. It is unclear what sorting centers would do in case of a bomb or anthrax alarm[92]. Should they call authorities or announce evacuation every time the alarm goes off? Or should they carry out additional screening while knowing that they are potentially dealing with something lethal? The former response protocol would be highly

[91] Monetary cost of security per mail item equals total costs of expenditures on purchased control equipment, installation, maintenance, staffing, and training.

[92] Recall that in Switzerland, the discovery of unidentified white powder resulted in the evacuation of the Zurich-Mülligen sorting center and delayed delivery of 1,5 – 2 million postal items over next few days.

disruptive to the postal service and burden unnecessary authorities that would be busy taking care of all false alarms. The latter response would evidently jeopardize the employee safety.

Another problem is that it is unclear for what purpose the postal traffic would be screened in the sorting center. The Swiss national civil aviation security program obliges Swiss Post to arrange security and safety screening for airmail. But outside the airmail domain, Swiss Post is free to decide whether additional screening is needed for certain product types, routes, or customer segments. The case study description revealed that Swiss Post screens currently voluntarily only imported parcel-size items, which their customs brokering staff must open in the import declaration process, and mail to business clients, which have purchased additional mailroom security services from Swiss Post. Otherwise, risk assessment, "likelihood times consequences," has determined that no further explosive screenings are necessary in the prevailing risk situation. As for contraband, Swiss Post is not much concerned screening for illegal traffic through the postal service, as long as the contraband does not endanger employee safety. It is the customs, the police, possible other law enforcement and regulatory agencies, which have interest to control the postal traffic contraband and security threats. However, it is unclear whether the authorities have interest to control the postal traffic contraband or security threats in the sorting center environment. The systematic mass screening would be in fact against their current risk-based approach of controlling only the highest risk segment of the postal traffic.

It is very challenging to integrate screening solutions into the high-velocity mail sorting process. Non-intrusive imagining technologies, colloquially called the X-ray machines, are maybe the most commonly applied solutions in contraband and security threat screening. The problem with these imagining techniques is that they need considerable time to produce a clear inside view of an object. These technologies therefore fit poorly the sorting center environment where conveyor belts move postal items at a constant speed of 2 m/s through the sorting process. Similarly, this velocity is far too fast for modern material trace detectors to perform screening accurately. The unavoidable fact is that without groundbreaking *automatic* threat detection innovations it is unlikely that any inline screening devices can be integrated into the sorting process in the close future. In fact, only free running detection dogs, radiation detectors, and other area screening methods, that are able to control a (storage) space for threats or contraband at once, might be used efficiently in the sorting center environment. But the area screening should be conducted while postal items are idle waiting sorting to begin or connection transport to leave the center. It is not certain, however, whether the items always wait idle long enough so that screening could be conducted.

Let us consider the special case of screening airmail already in the sorting center environment. Apparently, the airmail screening in the sorting center would make most sense because Swiss Post is obliged to arrange screening for the airmail in any case. The first problem with the

airmail screening in the sorting center environment is the reliance of the screening on X-ray imaging technologies, which as shown earlier, do not work accurately in the high-velocity sorting process. The other problem is that the standard postal logistics process is not as "airtight" as required by the airmail security regulations of the EU aviation security area. First, sorting center personnel is not trained, supervised, and vetted the way the regulations dictate. Moreover, secured "identifiable" airmail is not separated from surface mail, and it is not protected from tampering and mixing with the surface mail items and non-secured airmail from the moment of screening until it is loaded onto an aircraft's cargo hold. Also, the physical security measures at sorting centers tend to be inferior to those at the airports, and they do not likely meet the high aviation security standards. And finally, the carriage of postal items from post offices to the sorting centers and further to the airports does not always meet stringent aviation security requirements. "Even if we controlled the goods at the counter, I cannot exclude the possibility that someone would put something dangerous into a parcel during transport," the security manager of Swiss Post points out. "We have no guards, nothing." In his view, "the airmail exchange offices should be the only places where we conduct airmail security and safety checks. There we have technology, processes, and expertise we need." Another problem in the sorting center is that by the time of sorting, it not always sure which items are going to take a plane and which not. This uncertainty stems from the fact that routing and the mode of transport may change after the sorting center due to contingencies in airmail logistics, (e.g., overbooking, delays, and cancellations) or need for expedition of late items by air. The inability of distinguishing airmail as the sorting begins implies that, if the screening were conducted for the aviation security purposes, virtually all foreign-bound items should be screened. The unsegregated airmail screening would be not only unnecessary but it would also create a major customer service problem because aviation safety threats (e.g., perfume bottles) should be confiscated also from non-airmail items.

6.4.3. Redesigning of surface parcel screening

Since March 2011, when a parcel exploded in the office of SwissNuclear in Olten, Swiss Post has been screening foreign-origin surface parcels for explosives if the parcels are opened as part of the import clearance. In the current procedure, Swiss Post screens the to-be-opened parcels in a dedicated screening facility, which is located outside the mail exchange office. Due to the off-site screening facility, the parcels take a detour that delays their delivery for one day. The case study evidence suggests that this detour might be avoidable. If Swiss Post screened the parcels with material trace detectors instead of the X-ray equipment, the daylong detour to the off-site screening facility could be avoided. The trace detectors allow rather accurate on the spot screening of most explosive substances. Although the trace detectors might not be as accurate screening devices as the X-ray equipment, the accuracy would nevertheless be sufficient. A

negative reading from the trace detector would warrant sufficient confidence that the screened parcel does not contain explosives and detonate upon opening. In case of a positive reading, the parcel would be sent to the off-site X-ray facility for a decisive secondary screening, which would determine whether the true nature of the initial alarm (i.e., false or true positive). The primary screening with the explosive trace detectors would speed up the import clearance and the postal service in general because most parcels would no longer need to make the delaying detour to the off-site screening facility. An additional security benefit of the explosive trace detectors is that the devices can often be adjusted to detect materials also other than explosives. Expanding the library of the detected substances to cover a range of biological and chemical threats, which can be as harmful as exposives, would clearly increase protection the screening offers to the Swiss Post's customs brokering staff who need to open the parcels. Figure 24 presents some exemplars of the material trace detetors.

Safran Morpho, Hardened MobileTrace®

Rapiscan Systems®, HE50

Figure 24 Examples of trace detectors[93]

6.4.4. Postal service and the "secure supply chain" concept

The EU aviation security rules decree that all cargo and mail must be screened up to EU standards before being loaded an aircraft taking off from any EU airport (including Switzerland, Iceland, and Norway). However, if certain conditions are met cargo and mail from a "secure supply chain" can be loaded onto an aircraft[94] without screening at the airport. The secure supply chain concept is underpinned by the regulated agent, the account consignor, and the known consignor programs, which are maintained by the DG MOVE of the European Commission at the EU level and national civil aviation authorities at the member state level. Today, postal operators in countries following the EU aviation security regime, do not exploit

[93] Other major manufacturers include Smith Detection and Nuctech.

[94] Mail originating from account consignors can be loaded only onto all-cargo planes without screening at the airport. Mail from known consignors is perceived safe enough for transport also aboard passenger planes.

the possibility to load postal items from known consignors (KC) and account consignors (AC) without additional screening at the airport. This observation is somewhat inconsistent with the literature findings that suggest that sometimes upstream cargo inspections speeds up logistics and improves security. This inconsistency raises a question: why are not postal operators exploiting the opportunity the secure supply chain concept offers?

Let us start by summarizing the core principles of the "secure supply chain" legislation. The known consignor certificate is designed mainly for large, established shippers, especially large manufacturing companies. Therefore, the known consignors would be clients of the postal operators and never the postal operators themselves[95]. The known consignors are responsible for protecting identifiable air cargo and mail from unauthorized interference during production, packing, storaging, and staging for shipping. In particular, the known consignors must have adequate security measures[96] at their facilities and pay attention to security matters in staff recruiment, training, supervision, and other areas of human resource management. Once the known consignor is ready to ship out its airmail, postal operators would become responsible for protecting the airmail from (hostile) tampering and for preventing secured "clean" airmail from mixing up with not-yet-secured "dirty" airmail. Other in-transit security measures for identifiable, secured airmail include tamper-evident sealing and use of trained and reliable truck drivers. What is more, the high "airtight" security requirements should be followed through the entire postal logistics channel from the known consignor's factory gate to an airplanes' cargo hold. The problem is that the cost of meeting the high aviation security standards at every stage in the postal channel would be prohibitive and overweigh possible time and money savings resulting from avoided security screening at the airport. Another problem is that differentiation between regular and known consignor mail would necessitate a parallel mail handling process, which would further complicate the already complex airmail logistics. "We could exempt airmail coming from big, trusted clients from screening," the Swiss Post's manager indicates that Swiss Post indeed receives mail from known consignors but does not handle it anyhow differently than regular airmail[97]. "It is often easier to just screen everything."

The account consignor program is even less relevant for Posts and users of the postal services than the known consignor program. The lack of relevance stems from the fact that mail from

[95] Posts and other logistics service providers can apply for the regulated agent (RA) certificate that is intended for intermediaries that handle identifiable airmail.

[96] Known Consignor requirements overlap with the AEO-S requiremements to some extent. I cannot compare in detail official criteria for getting AEO-S and Known Consignor certificates because the validation checklist for known consignors, which specifies requirments applying the known consigor status, is published in a confidential commission decision (2010/774).

[97] It is likely that the mail volume from known / account consignors will increase in the future as more and more shippers obtain the certificates.

account consignors has the "SCO" security status (= secure for cargo aircraft only) and thus it cannot be loaded aboard passenger line flights that postal operators commonly use to move airmail. And even if the "SCO" airmail was booked to fly aboard an all-cargo air freighter, problems might arise later due to delays, groundings, booking errors, and other contingencies that force last minute flight changes. In case the "SCO" airmail ended up taking a passenger flight, the security status would need to be upgraded to "SPX" (= secure for passenger and cargo aircraft) through screening. As the "SCO" status reduces the flexibility of the airmail logistics, it is not a reasonable choice from the logistics viewpoint. Another problem is that the "SCO" status does not make security sense either: as crewmembers may die on both passenger and cargo flights, and plane crashes may kill unexpecting people at the ground, especially at densely populated urban areas, it is questionable to accept less stringent security for all-cargo flights than for passenger flights. Perhaps the only way how the postal sector could benefit from the known consignor and account consignor programs is associated with the new pre-loading advance electronic information (AEI) requirement the European Commission is intruducing as part of the new Union Customs Code (UCC). To reiterate briefly, the pre-loading principle means that customs receive information on airmail items before they are screened or loaded aboard an airplane. The advance information allows the customs to calculate a risk score and select those items that with the highest risk scores to extra intense high-risk cargo and mail (HRCM) screening. Now, if the customs' risk scoring algorithms considered known consignor status as a sign of trustworthiness, the mail coming from the known consignors would face the extra intense screening less frequently than regular airmail items.

6.4.5. Digitalization and sharing of X-ray images and other control evidence

Over the recent years, digitalization of logistics information has been one of the most influential trends in the logistics industry, across all modes of transport. The EU's Customs 2020 strategy and the new Union Customs Code (UCC) both endorse digital, computerized information sharing between and among customs and trading companies. In the air cargo and mail domain, the IATA's "e-freight" initiative and the namesake EU research and development project have been developing and demonstrating solutions of the paperless logistics. Also in the postal sector, there has been numerous digitalization projects that have reduced the dependency of the modern postal logistics from the paper documents. Most importantly, the UPU has designed a series of EDI messages that are equivalent to the UPU's standard CN documents, that have served decades as the backbone of international postal logistics communication. In practice, the Postal Technology Center (PTC), "the operational arm of the Telematics Cooperative" of the

UPU, manages the Post*Net platform[98] that provides technical infrastructure for a secure and standardized global EDI messaging among "Posts, airlines, carriers, customs authorities, security agencies and any other transport and distributions organization anywhere in the world" (PTC 2013). Meanwhile, the International Post Corporation (IPC) has been and is still engaging in "e-freight" initiatives, as well. Its two most notable projects include the Future of Mail by Air (FoMbA) on digital information exchange between Posts, airlines, ground handlers, and customs authorities and the Mails Electronic Data Interchange and Customs Integration (MEDICI) on building a platform for efficient transmission of electronic item-level data[99] from the origin Posts to the destination Post.

So far it seems that the digitalization trend improves productivity of the postal logistics processes. The digital data enables faster and more automatic information processing and sharing, and enables large-scale information storage for business intelligence purposes. The timely digital information also holds a promise of increasing visibility over the postal logistics chain, thus making the postal operators more capable of detecting and responding to logistics contingencies. In addition to rather obvious logistics benefits, the e-freight concept could be stretched a bit further, to cover also security information. In theory, authorities and postal operators could digitalize X-ray images, sensor data, and other control evidence they generate through security and customs controls. The digital control evidence would be relatively easy to share among concerned parties and to archive for future analysis.

The archived digital control evidence would facilitate crime investigations tremendously. After a plane crash, for instance, accident investigators could re-examine archived digital images of cargo and mail items aboard the crashed flight. In the post hoc re-examination, the investigators might detect the explosive device, which very likely destroyed the plane and caused the crash. Knowing the exploded item would enable the investigators to trace its origin down to a specific country, city, or even postcode area or a public mailbox[100]. This geographic clue would speed up the investigations and allow the authorities to restrict flight bans and other precautionary measures to certain high-risk countries and airports, and this way avoid disrupting the entire

[98] The Post*Net enables sharing of tracking events across the international postal system, among many other features. It should be noted, however, that not all postal operators use the UPU's IPS. Especially Posts in industrialized countries use more functional and flexible solutions to manage their operations. But fortunately, although the many logistics information systems that the postal operators use, the systems are often capable of communicating with each other thanks to standardized, compatible EDI messaging systems.

[99] The item-level data is sent in the ITMATT EDI message, which digital contents corresponds largely the data elements in the UPU's CN23 customs declaration form.

[100] It is common that airmail from all around the world gets mixed at major transfer airports. So while inbounds flights may carry items from a single country, outbound flights, taking off from the transfer hubs, invariably have mail from multiple countries aboard. This mixing of airmail at the transfer hubs complicates investigations of potential mid-air plane bombings. Even if investigators would indicate an explosion in airmail cargo hold as the most probable cause for an accident, currently, without digital archives of the X-ray images, it is nearly impossible to pinpoint the specific postal item that caused the blast.

postal service. As the second benefit, the re-examination of the digital X-ray images would reveal authorities how the explosive item was assembled and concealed, thus helping them to design more effective future air cargo and mail screening systems.

Further benefits from the digitalization of the control evidence would arise if the controllers shared the digital control evidence with each other. Recall that many screening methods, especially the X-ray imaging technologies, are capable of detecting many types of contraband and security threats. Remember also that in the airmail security and safety controls, although the multi-threat X-ray imaging is commonly used, the screening targets only aviation security and safety threats – explosive and incendiary devices capable of destroyng a plane. Due to this narrow focus, undeclared contraband often passes the X-ray screening as long as the contraband does not endanger aviation securit and safety. Remarkably, customs officers in the country of destination could reuse the digital X-ray images, that have been inititally taken for the aviation security and safety purposes, to search for undeclared contraband, such as illegal drugs, undeclared tobacco, CITES goods, and counterfeits[101]. What is more, the customs could re-examine the X-ray images even *before* the airmail arrives in their territory. The early availability of the digital X-ray images would allow the customs to use the visual evidence (the X-ray images) to make better decisions about what shipments to select to customs controls. More precisely, the images would be consequential input to the customs' pre-arrival risk assessment. Ideally, it would allow the customs to contrast the visual X-ray evidence against the pre-declared contents of the items received as part of advance electronic information (AEI) datasets, thus resulting more accurate risk assessment and more effective inspections.

The idea of sharing and re-examining of the digital X-ray images involves certain technical and political problems. One problem is that while X-ray operators can change intensity and angle of rays for higher clarity and resolution, a digitally reconstructed X-ray image provides only a static representation. Another technical issue is that even if the X-ray machines were able to produce digital images, given the size and the quantity of image files, transmission of the X-ray control evidence would require high capacity broadband links between the sender and the receiver. In one future scenario, the screening operator would annex the digital X-ray images into the electronic consignment security declaration (e-CSD). This would be a relatively simple way to share the control evidence because screening operators (or regulated agents in general) must issue consignment security declarations in any case as soon as they have secured a shipment and granted it a security status. However, as regulated agents currently provide the

[101] According to the same logic, the customs in the country of destination might benefit from the digital evidence generated through export and transit controls (e.g., targeted contraband, applied technique(s), findings, and the digital evidence, such the X-ray images). However, because in the postal traffic, the export and transit controls are rare whereas airmail security and safety screening are systematic, transferring digital X-ray images from the airmail security screener to the customs in the country of destination would bring the largest benefits.

CSD information only to aviation security authorities on request, one hurdle to overcome is to make this information available for the customs and other border control agencies, as well. Thus, the vision calls for close collaboration between the transport security and the customs authorities, especially at the global WCO, IATA, and ICAO levels.

6.5. Collaboration & culture

The theory and the practice of SCS management strongly suggest that government-post collaboration is instrumental for effective and logistics-friendly security. The case study evidence showed that there might be room for improvement when it comes to collaboration between Swiss post and Swiss law enforcement agencies and between Swiss Post's management and work force.

6.5.1. Challenges in government-post interaction

The nature and extent of business-government collaboration in the Swiss postal logistics context seems to be less intense than I expected before conducting the case study. When asked how Swiss Post could help the Swiss customs to tackle smuggling, the tax specialist from Swiss customs corrected that Swiss Post "is not actually helping" the customs as much as they are complying with legal requirements. "Customs set the rules and they [Swiss Post] have to follow them." The view on the customs-post interaction appears to be reciprocal. "It's not about how we can help the police or the customs to do their job," the representative of Swiss Post asserts, implying that Swiss Post fulfills its regulatory requirement but otherwise takes a back seat. Certainly, over the past decades, Swiss Post has been more and more fostering relationships with relevant Swiss authorities, and the authorities have become increasingly willing to communicate and collaborate with Swiss Post. But still, it seems that there is some room for improving the post-customs collaboration. Practitioners argue that we can pursue the more intense collaboration through co-creation of rules and bi-directional education. The co-creation is about preparing laws and regulations in a process where business and governmental actors develop requirements bottom-up through a mutually respective dialogue. For the effective and efficient co-creation, it is crucial for the postal industry to speak with one voice, for example through the Universal Postal Union or its regional affiliate organizations such as PostEurop. The postal industry should maintain dialogue with the European Commission, the World Customs Organization (WCO), International Civil Aviation Organization (ICAO), International Air Transport Association (IATA) and other relevant international bodies that are interested in customs and security matters. The bi-directional education is about sharing and understanding one's interests, objectives, and limitations. The postal industry, for instance, should always explain authorities, policy makers, and regulators special characters of the postal service, particularly the Universal Service Obligations and the huge volume of postal items.

6.5.2. Postal service and AEO-S program

Posts eligibility to the EU AEO programs (security / full[102]) is one of the key question marks in the new Union Customs Code, which requirements are expected to become gradually applicable by 2020. The current "old" Community Customs Code grants AEO-S and AEO-F certificate holders benefits that simplify their compliance with certain customs security formalities: the holders have right to use a reduced data set for entry and exit summary declarations[103] and they have the possibility to get prior notification of customs controls. Most likely, to encourage more companies to join the EU AEO program, the new Union Customs Code is going to introduce further AEO-S benefits that streamline cross-border traffic, including earlier release of goods to free circulation and an extended period of temporary storage. Aside the development of the Union Customs Code, the European Commission is negotiating "mutual recognition" agreements (MRAs) that might bring some benefits for EU AEO certificate holders also outside the EU customs security area. The mutual agreements also are also likely to boost international reputation of the certificate AEO-S holders as a trusted, quality economic operator.

In the past, postal operators have not been keen to apply for the AEO-S certificates mainly because the old Community Customs Code (CCC) exempted the postal traffic from the AEI requirement, and thus the certificate would have not benefited the Posts. But today, when the European Commission is about to revoke the AEI exemption from certain segments of the postal traffic and introduce new benefits for AEO-S certificate holders, the AEO-S status becomes beneficial for the postal operators. Yet, it is still unclear whether the postal operators are eligible for the AEO-S certificate. The current EU customs legislation, in brief, states that applicants of the AEO certificates[104] must have an excellent track record of customs compliance, be financially solvent, follow good accounting practices, and comply with a set of security measures. The concern on the Post's eligibility for the AEO certificate arises from the latter security provision, and particularly the following requirement: "the applicant has implemented measures allowing a clear identification of his business partners in order to secure the international supply chain." Recall that Swiss Posts and other "designated operators" with Universal Service Obligations (USO) are responsible for offering basic postal services for everybody throughout their national territories. Because of this responsibility, Posts receive postal items from a large number of senders, many of whom are ordinary people who Posts do

[102] This section talks about the AEO-F and AEO-S programs that make certified companies eligible for simplified security compliance. The AEO-F status includes besides the AEO-S status also AEO-C (customs) status, which provides customs facilitation benefits for the certificate holders.

[103] Recall that the exit and entry summary declaration (ENS and EXS) are the AEI data set in the EU customs security area.

[104] It is worth to note that the Swiss AEO program concerns to border security controls, not customs controls. When contrasting to the EU customs compliance programs, the Swiss "security-centric" AEO corresponds the EU AEO-S certificate. The Swiss Authorised Consignee and Authorised Consignor programs resembles the EU AEO-C certificate.

not know and who do not have a track record of customs compliance. The multiplicity of senders and open nature of the postal makes it impossible to identify each sender "in order to secure the international supply chain."

Now, postal operators are wishing that their inability to identify all their business partners (the senders) would not prevent them from getting the AEO-S status and enjoying its current and expected benefits. Good news for the postal industry is that the widely recognized WCO's SAFE framework standards stipulates that "customs should provide equal access to simplified arrangements to AEOs regardless of the mode of transport." Also, in the most recent 2012 edition of the EU AEO guidelines, DG TAXUD, the responsible EU body for the AEO program, recognizes the particularity of the postal service. The guidelines imply that a large traffic volume should not be a barrier for the AEO-S certification: "the number of infringements related with customs declarations should always be examined and compared to the total number of transactions […]." Moreover, the AEO guidelines highlight the importance of vetting backgrounds, supervising, and training of current and prospective postal employees. The guidelines also remarks, although vaguely, that the AEO certified companies should take "appropriate measures" to lower the security risks of unknown shippers to "an acceptable level." So far, this recognition in the AEO guidelines has not influenced the EU's formal regulatory framework on customs security. The current legislation[105] states plainly "the customs authorities shall take due account of the specific characteristics of economic operators." There is an urgent need[106] to specify what requirements the postal operators should meet in order to get AEO-S certificate. Perhaps approach would be to include the criteria in the next edition of the EU AEO guidelines.

6.5.3. Future regulation and standardization

The case study reveals that authorities regulate the postal security management mainly in the aviation security and customs security domains. The airmail security regime in the EU, being stringent, detailed, and strongly enforced, leaves little room for postal operators to use their own discretion and interpretation. Likewise, the export and import procedures of international exchange of postal items are defined in detail in the Community Customs Code and its implementing regulations, a volume spanning over thousand pages. On the contrary, to date, anti-theft and surface mail security, among other areas of postal security, have remained mostly

[105] Regulation 1875/2006, Section 1, Art. 14a(2).

[106] The specification should be done fast, before the requirements of the new Union Customs Code become applicable, so that Posts can apply for and receive AEO-S statuses well before the new legal AEI requirements become applicable in the postal sector.

unregulated[107]. The question is whether governments should extend their regulatory control beyond the customs security and aviation security.

Perhaps we should start regulating how postal operators prevent and investigate mail theft. The case study evidence suggests that mail theft is predominantly a consumer right issue and thus a key concern for postal regulatory authorities and users of the postal service. In Switzerland, Swiss Post is already doing much to prevent and investigate mail theft, which is evidenced by consistently low mail theft rates. With respect to theft, the yellow giant shares the same attitude than many logistics service providers in other industries: "We present the interest of our customer, so we are very interested in reducing stealing to minimum," the Swiss Post's security manager explains. "We have a moral obligation to do something. That's part of our service." Notably, when contrasted against the multibillion-franc Swiss postal business, mail theft costs close to nothing for Swiss Post. This is because only a tiny fraction of mail gets stolen, and because an average reimbursement for a lost item is relatively low (up to 150 CHF for international registered letters and up to 1000 CHF for international parcels). Therefore, rather than monetary losses, Swiss Post's strong commitment to theft prevention arises mainly from reputational and employee safety concerns: each lost items erodes public confidence in the postal service, and violent mail thieves jeopardize the work safety. Because Swiss Post has a strong moral incentive to bring mail theft close to zero, there seems to be no need to regulate anti-theft postal security in the present day Switzerland and apparently elsewhere in Europe. However, the postal regulatory authorities, consumer watchdog organizations, and the governments should keep an eye on the postal service and reconsider regulatory intervention if they saw mail theft rate soar in the future. To conclude, it seems that the way to go in anti-theft postal management is to identify best practices for preventing, detecting and investigating theft in the postal network. It is clear that many postal operators are very interested in fighting theft and thus consider anti-theft solutions as an important domain of the postal security management. It is also safe to assume that the postal organizations worldwide have accumulated a great deal of experience and knowledge on mail theft prevention and investigation. It would beneficial for the postal community as a whole if the anti-theft know-how were compiled into a single best practice guidebook. Major postal organizations such as UPU, IPC, and PostEurop could take the initiative in producing the anti-theft guidebook of the postal service. Maybe eventually, the most useful best practices could be integrated into the UPU's security postal security standard (S58).

Another loosely regulated area is the security of the surface postal traffic. Certainly, transport authorities regulate transport in dangerous goods, and the customs monitor and control cross-

[107] Since the 25th Universal Postal Congress, in Doha, Qatar, in September/October 2012, "general" minimum security standards have become mandatory for Posts worldwide. The standard covers partly also the theft prevention domain.

border traffic across modes of transport to detect and eliminate chemical, biological, nuclear, radiological, and explosive (CBRNe) security risks. But surface postal traffic is rarely subject to any security checks by any authority, especially the domestic Swiss traffic, the intra-EU traffic, and the EU-CH traffic. If authorities rarely inspect the surface postal traffic, perhaps Posts themselves should be legally obliged to screen the cross-border traffic for the security threats. Interestingly, the case study evidence shows that Swiss Post is already screening imported surface parcels for explosives, if the parcels need to be opened in the customs clearance process. Moreover, Swiss Post offers supplementary mail screening service for clients, mainly banks and government bodies, which seek extra protection against mail bombs. To conclude, Swiss Post is already screening surface mail as appropriate to protect their employees (and their colleagues at the customs) and to meet needs of their security-concerned clients. It seems that, under the current security environment, where no immediate terrorist threats exist, there is no need for stepping up security screening of the surface postal traffic in Switzerland.

One policy area that might require additional regulatory oversight is critical infrastructure protection (CIP). Because failures or disruptions of postal (and courier) services might lead to substantial economic and social losses, many countries have designated the postal system as national critical infrastructure. The designation recognizes the fact that the reliable postal service is a matter of necessity rather than convenience: disruptions in the postal service may damage commerce, undermine public administration, jeopardize patient safety, and weaken the governments' capability to respond to emergencies. In Switzerland, the Federal Office for Civil Protection (FOCP) is responsible for liasing with and overseeing Swiss Post and its capabilities to prevent, resist, and recover from disasters and major contingencies. In its basic strategy for critical infrastructure protection, FOCP designate the postal (and courier) service as one of the 31 sub-sectors that has a national importance, giving it a "high" criticality status at a three level scale, two other statuses being "regular" and "very high" criticality. Considering the importance of the postal service to the Swiss society (see Box 13), FOCP might need to consider regulating[108] Swiss Post to reduce the exposure of the postal service major hazards.

1) Enabler of competitive business models

The postal service enables business models that involve shipping of small shipments of physical products directly to consumers' homes (e.g., mail order retailers, online auction sites, and press houses). Posts also handle the reverse flow of returned, damaged, and outdated products from customers back to manufacturers and retailers. Besides, the postal service provides fast and simple access to foreign markets, especially for small and medium size enterprises (SMEs).

[108] The regulation might need to oblige Swiss Post to maintain spare sorting capacity, have reserve vehicles, set up back-up IT systems, cross-train postal workers, and set measures to shield the postal system from failures of other critical infrastructures (e.g., power generators and fuel reserves).

2) Reliable messenger

The role of Posts as messengers has been rapidly diminishing in the information era. However, the postmen and couriers still facilitate communication between citizens, authorities, and businesses by carrying contracts, patent applications, diplomatic correspondence, exams, votes, visas, passports, love letters, and many other documents. In fact, Swiss Post still delivers on average 18,8 million letter-size items a day in a country of around 8 million inhabitants. Moreover, the physical "snail mail" plays a particularly important role as a back-up communication channel if electronic means of communication fail.

3) Courier of time-critical supplies

Swiss Post and its subsidiary TNT Swiss Post offer expedited delivery service for time-critical goods and documents. The health care sector, where timely deliveries can be a matter of death and life, for example, use the expedited services to transport medicines, laboratory samples, blood, and other medical supplies. Critical spare parts are another example of time-critical products. Organizations across industries, in particular airlines, power plants, automobile manufacturers, and armed forces, rely on fast spare part deliveries to minimize costly downtime of operations. Short transport times are crucial when shipping perishable consumer goods like fruits, fish, and flowers.

4) Aide in emergency logistics

Authorities could exploit the nationwide postal and courier networks to organize emergency logistics. The postal systems, for example, could distribute antidotes to the entire population within 24 hours to contain spreading of a contagious disease in the event of a bio-terror attack or a pandemic outbreak. The postmen and the couriers could also contribute to relief logistics missions by delivering food, shelters and medicines into disaster zones as soon as conditions allow safe operation.

5) Accelelator of military mobilization

The defense forces could use the postal network to call citizens to arms, especially when a surprise attack has disabled electronic means of communication. The postal and courier networks could also supply a countrywide militia with weapons and ammunition. The supply of ammunition by mail could be a strategy in Switzerland where many male citizens keep their military weapons but no shells and ammunition at home.

Box 13 Five reasons why the postal service is critical for the Swiss society[109]

Besides introducing new regulations, some areas of postal security and customs matters might benefit from more *relaxed* regulations. One way to streamlining the import declaration process, for example, is to leave additional segments of the postal traffic outside import declaration requirement or expand the range of items that are eligible for simplified customs declarations. Fewer and simpler import declarations would clearly alleviate Post's burden and speed up the cross-border mail flow. The issue of simplified customs formalities relates also to the discussion

[109] Adapted from my own article that was published at Network Industry Quarterly, 15*(4)*, 16-19.)

about raising minimum levels of taxes and duties authorities collect, so called tax deminimis thresholds. The increase in the tax deminimis would speed up cross-border logistics and reduce costs associated with the customs clearance. The higher tax de-minimis thresholds would not decrease significantly taxes governments collect through the customs because, for example in Switzerland, taxes raised from the postal traffic are just a few million francs per year, a tiny fraction of the total tax revenues the Swiss customs collect.

Regulations aside, would the postal industry benefit from additional standardization of the postal security management? The international postal service is a collaborative effort where originating and receiving postal operators exchange mail items, often through one or more intermediate Posts that forward mail through their territories. Each UPU member exchanges postal items with every other 191 UPU members, either directly or through the intermediary posts. Since its inception in 1874, UPU has been working towards faster and more efficient cross-border postal logistics through worldwide standardization and capability building. The persistent standardization efforts have no doubt benefited the international postal service tremendously. Even so, not until late 2010, when the Yemen bomb plot raised concerns of airmail security and prompted top-level politicians and authorities call for "minimum security standards" for the postal industry, there have been only limited attempts to standardize the postal security management. Soon after the Yemen bomb plot, the heightened security concerns resulted into the development and worldwide adoption of the UPU's two security standards, one on the general postal security (S58) and another on the airmail security (S59). Other standardization projects were launched as well. In the EU, a four-year demonstration project SAFEPOST was started, with goal of designing, demonstrating, and standardizing general security solutions for securing the international postal service. Also IATA has been developing a global for the electronic consignment security declaration (e-CDS), which digital or paper-based version must be issued when a regulated agent grants a security status to an airmail shipment after security and safety screening. But despite these projects, the standardization of the postal security management is still in its infancy.

The UPU's two postal security standards are far the most important postal security standards to date. Nevertheless, a close scrutiny of the standards reveals that the requirements of the both standards are rather rudimentary. It is questionable whether the airmail security standard (S59) adds anything new to the airmail security anywhere. The fact is that all UPU member countries, expect for one, have signed the ICAO's Chicago Convention, which Annex 17 sets baseline rules for global airmail security. These ICAO rules seem to meet or exceed the standards laid down in the UPU standard[110]. And certainly, the UPU's airmail security standard makes no difference in

[110] The Annex 17 uses much moderating phrases and ambiguous terminology, making it hard to understand exact airmail security requirements. More detailed guidance for implementing the general principles are laid down in a confidential dossier called

the EU security area, where a stringent and detailed airmail security regime is already followed[111]. The UPU's two standards affect security perhaps only in the least developed parts of the world where postal operators have not yet adopted some of the advanced airmail security concepts, such as the designation and screening of high-risk cargo and mail (HRCM)[112].

But if the standards add something new into the existing postal security practice in theory, it is not sure whether they do so in practice because there is currently no compliance monitoring program in place. Therefore, the next logical step in the standardization is to launch an auditing / compliance monitoring program. It is true that the UPU's general security standard on physical postal security (S58) obliges Posts to carry out annual self-audits, conducted by "appropriately" trained people who are independent of those responsible for implementing the standard. However, the main problem is the lack of external compliance monitoring. In the absence of any external compliance monitoring mechanism, we do not know whether Posts, which did not already meet the requirements of the two postal security standards, are now making serious and productive efforts towards better compliance. This is critical because there is always a risk that postal operators either neglect some standards or misinterpret them the way that best fits their business interests. "Regulations might be designed by people who do not know your business," a postal manager explains his attitude towards top-down regulations and standards. "You must have somebody who can translate expectations into applicable solutions."

Setting up an office of external independent auditors would alleviate the problem of compliance monitoring. The group of objective auditors, who would use common criteria, would be a way to ensure harmonized and adequate implementation of the UPU's postal security standards throughout the universal postal territory. Ideally, the external auditing program would also have funds to help underperforming Posts to build necessary security capabilities, including IT systems, management know-how, and trained personnel. The office of auditor should also have power to incentivize and sanction Posts to comply with the requirements of the two UPU postal security standards. For the maximum effect, to courage consistently high performance of the postal operators, the auditing should be conducted in relatively short intervals (to prevent

---

Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference. Therefore, without access to this document, I could not analyze whether the detailed security measures would go beyond the requirements of the UPU's airmail security standards.

[111] The UPU's airmail security standards do not affect security of flights taking off from airports belonging to the EU aviation security area. Neither do the standards affect the security entering the EU aviation area because of the ACC3 (Air Cargo or Mail Carrier operating into the Union from a Third Country Airport) regulation that since 1 July 2014, has been forcing airlines flying from third countries into the EU to apply airmail security measures equivivalent to the measures applied in the EU aviation security area.

[112] An item is designated as high-risk if it has signs of tampering, tactical intelligence has red-flagged it, the shipment comes from or transits through a high-risk country, or due to its special packaging, the shipment calls for special screening.

deterioration of the security system) and unannounced (to prevent shirking from security duties). The purpose of the sanctions and the possible unannounced audits is to create a credible threat for companies, which fail to comply with the regulations.

Later, another important step to take in the compliance monitoring is to shift the focus of the auditing from measuring nominal level of security implementation (e.g., how many percentages of the requirements has the postal operator adopted?) to measuring the actual security performance (e.g., how many percentages of security threats the security system detects and intercepts?). This shift is crucial because the causal relationship between the level of implementation and the actual performance is not necessary linear, significant, or even positive. In other words, a security compliant company is not always more capable of detecting or intercepting crime than its non-compliant peer organizations. But how could we measure the actual security performance of the postal system? One solution to the performance-based auditing is to conduct red-team attacks, in which a group of security experts tests the current security defenses in a simulated attack. However, even the red-team attacking is not ideal measurement technique because it measures only the system's ability to detect and intercept illegal activities, not its ability to discourage crime or support criminal investigations[113]. The box 14 presents one idea of establishing a performance-based auditing system in the cross-border postal network.

There might also be need to standardize conventions for recording and reporting crime and terrorist incidents in the postal network. Such recording and reporting standards would allow establishment of an international postal crime database that would ideally guide future policy making regulating, and management of the postal security. The database would also allow of benchmarking of security performance across countries. Moreover, the previously described performance-based auditing system would benefit from a standardized crime and security incident reporting conventions.

[113] The interception rate for mail bombs, for example, can be calculated based on the percentage of inert test bombs that pass the screening undetected.

The International Post Corporation has run an RFID-based UNEX system for tracking of international priority letters already since 1994. Around 4500 volunteers keep the UNEX system in operation by sending around 500 000 RFID-tagged test letters a year according to a mailing plan, which reflects regular patterns of the international postal traffic. Registration gates of the UNEX system, erected along the mail pipeline at regular intervals, register time and location of the test letter, which otherwise would be untrackable because they travel without barcode identifiers. The tracking data reveals average lead times for various sections in the mail pipeline, helps pinpoint bottlenecks in the postal logistics system, and enables performance monitoring of the international postal service in terms of delivery speed. In theory, the UNEX infrastructure could be harnessed also for security performance monitoring. If the test letters were loaded with inert explosive devices, we could observe the percentage of the inert threats passing aviation security screening and other possible explosive controls in the postal logistics network. With the same logic, the senders could load the test letters with other types of contraband, let say narcotics, to test effectiveness of border controls. Apparently, leveraging the UNEX system for the security performance measuring involves operational challenges: How to ensure that the inert explosives do not trigger evacuations and other emergency maneuvers whenever they cause alarms? How to simulate the diversity of homemade, improvised explosive devices in terms of size, materials, and shapes? Which entity would be responsible for overseeing the security performance monitoring program?

Box 14 Application of the UNEX mail tracking system in security performance monitoring

6.5.4. Security-centric human resource management

Staff plays a crucial role in all areas of postal security, as Swiss Post's security and safety manager succinctly summarizes: "You can have structural, organizational, and technical security measures. But finally, the weakest link is the human itself." The staff plays actually three roles in the postal security. In the role of a protagonist, the personnel fight against crime: they stay vigilant to suspicious activities, follow security procedures, and aid investigations. But unfortunately, big organizations like Swiss Post are bound to hire some dishonest individuals. The dishonest staff members play the role of antagonists who use their insider information to commit crime themselves, or they help external people to do so. Thirdly, and most sadly, the staff members fall victims to robberies, mail bombings, and other types of assaults taking place in the postal context. The central role of people in postal security, as the defenders, antagonists, and the victims, raises questions about human resource management in the Swiss Post's organization. The following sections analyze some burning issues of security-centric human resource management in the postal logistics network, which arise from the literature synthesis and the case study description. The intent of this analysis is not to repeat the guidance already presented in the UPU's two postal security standard, which largely covers important human resource management aspects such as background vetting of job candidates, security awareness

building, work contract termination procedures, and provision of channels for reporting suspicious activities and misconduct.

The literature synthesis revealed that commonness of part-time and outsourced workers might affect security negatively. The temporal people have less to lose than permanent employees, who have their relative secure jobs and possible career ambitions at the stake. Therefore, the temporal workers have weaker incentive to respect security procedures and stay vigilant. The case study interviews seem to corroborate this argument. "Part-time workers might not adopt security culture, awareness, and understanding the way they would if they had a fixed, secure jobs," the Swiss Post's manager assumes. "These people might never feel involved with the Swiss Post and its values," he goes on to point out how part-timers might feel alienated from the Swiss Post's security culture. If the statement holds true, Swiss Post faces a massive challenge: in 2013, Swiss Post employed nearly 62000 people, of whom around 49% worked part-time. He also presumed that the lack of commitment to Swiss Post's values and culture might also apply to outsourced workers. "Last week, Swiss Post decided to cut 250 jobs in the transport function. I understand this from the economic point of view: we pay more for our own drivers than for the drivers of third parties. But from the security perspective, are those third party workers as reliable as our own employees? […] Do these people think of and care about security?"

Another factor affecting security is the relatively small salaries among the ranks of lowest earning staff. In a recent case from the beginning of 2014, Swiss Post's two part-time sorting center workers were convicted for stealing goods worth around 100 000 CHF from postal parcels. Once finally caught after months of investigations, the thieves justified their crime with inadequate salary. Besides this anecdote, we learned from the literature review that low the remuneration often makes it difficult to attract and retain competent and motivated workforce (Belzer and Swan 2011). The resultant high turnover and poor motivation undermine efforts of maintaining trained and vigilant staff that is committed to security objectives. Besides, by paying very low salaries Swiss Post might become the least preferable option for employment among blue-collar workers. In the worst case, the high turnover and the lack of good job applicants helps terrorists and career criminals to infiltrate into the postal organization. The obvious remedy to these problems is to increase compensation of the lowest earning staff. Moreover, aside the higher lowest salaries, Swiss Post could design monetary or other incentives to reward their employees for exemplary vigilance and proactivity on security matters.

The staff's preparedness to deal with emergencies is another key aspect of security-centric human resource management. Postal operators and authorities surely have plans for dealing with emergencies, but the staff's ability to execute these plans in a crisis situation is uncertain. The white powder discovery at the Zurich-Mülligen sorting center in Autumn 2012 is an

example of a situation when things did not go according to the plan. "A series of mistakes and wrong decisions lead to this situation," the Swiss Post's manager recalls the chain of events leading to the evacuation after the Zurich-Mülligen sorting center. First, the parcel broke accidentally revealing the white suspicious substance. Then, somebody at the sorting center called a wrong number at the police, and the receiver of the call didn't know about the agreement between Swiss Post and authorities that prescribes standard contingency procedures. In this case, the police should have picked up the unknown white substance discreetly, brought it to a cantonal laboratory for analysis, and decided countermeasures based on the test results. But instead, the blue light organizations dispatched 25 police cars, 25 ambulances, and numerous firefighter units immediately to the sorting site (see Figure 25). "That wasn't a planned procedure," he stresses adding that the disruption could have been avoided if the sorting staff had followed standard contingency procedures. Had the employees gone through preparatory emergency drills, perhaps Swiss Post could have avoided the ramifications of the Mülligen white powder discovery. Drills and other practical exercises would also save lives when actual emergencies occur.

Figure 25 Zurich- Mülligen white powder discovery

6.6. Summary of recommendations

This chapter applied the model of logistics-friendly logistics to the case study on the Swiss-centric postal logistics networks. This analysis revealed some opportunities for further improvement of postal security management and governance in Switzerland. This section restates the main findings and recommendations.

The case evidence suggests that in every studied domain of postal security management, the implemented security solutions were commensurate to the risk they seek to address. We found that Swiss Post does business as usual, without special security procedures, as long as there is no reason to step up security levels. The same applies to government agencies that do not dedicate much resources on postal security when they have no urgent reasons to do so. However, both Swiss Post and the government agencies recognize that the security threat

landscape could change in the future, so they maintain a degree of capability to respond to security contingencies, unexpected threats and more stringent (regulatory) security requirements. This capability could be further strengthened as follows:

- Invest in mobile resources, cross training of staff, and workforce reserve to deal with special security needs (new threats or more stringent security requirements) and security-related traffic congestions.
- Prepare and drill emergency and logistics contingency plans. For instance, what to do if biological weapons were found in the Swiss postal system.
- Develop technology and build expertise proactively to address security contingencies fast and cost-efficiently.

The secrecy of information was found to be another key issue in the postal security management. Among other things, we noted that on the one hand, indication of security-sensitive mail items seems reasonable so that staff can pay special attention to them. On the other hand, the indication helps potential criminals identify worth-to-steal items or terrorist-prone airmail items. Information about security solutions seemed also to increase the deterrence effect that, if high enough, would discourage criminals from attempting crime. But sometimes the very same information about the security solutions enables criminals to find and exploit weaknesses in the security systems. On these grounds, security information should be disclosed sparingly, paying attention to recommendations below:

- Conceal theft-prone items by removing indicators of high value (e.g., logos of high-tech companies), avoiding visible special anti-theft protections (e.g., security tapes), hiding postal items inside mail aggregates, and by converting written information into digital form that is illegible to the naked eye.
- Indicate terrorism-prone airmail items so that they would not mix them with less vulnerable items and so that the staff would pay special care when handling them.
- Communicate general principles of security procedures to reduce logistics uncertainty. Reserve right to unannounced controls, and alternate the security procedures once a while.
- Strip the postal service off layers of anonymity. Depending on the seriousness of the addressed security risk, consider introducing ID checks at post office counters, banning cash payments, or shutting down pseudonymous poste restante addresses or P.O boxes.

The analysis also identified some promising opportunities for integrating security controls into the baseline postal logistics process. Currently Swiss Post uses X-ray equipment to screen imported surface parcels that customs brokers open in the customs clearance process. The parcels get screened in an off-site X-ray facility, and the detour to this facility delays the delivery for one full day. If Swiss Post screened the parcels with material trace detectors instead

of the X-ray equipment, the daylong detour to the off-site screening facility could be avoided. As a bonus benefit, the material trace detectors could search for biological and chemical threats in addition to primarily targeted bombs. We also found that digitalization and sharing of security control evidence, X-ray images in particular, would increase accuracy of physical inspections in the downstream postal delivery channel. A digital archive of X-ray pictures might help speed up investigations in the aftermaths of mail bombing incidents. As another point related to the logistics integration, this analysis section investigated whether it is a reasonable to screen postal traffic centrally in sorting centers. We concluded that the sorting center screening is not reasonable due to a range of technical, political, and employee safety reasons. The following recommendations conclude the discussion on the integration of the security solutions in the postal network:

- Screen imported surface parcels with material trace detectors instead of X-ray equipment. The change of the screening technology would eliminate the need for the daylong detour to the off-site X-ray screening facility and offer extra protection against biological and chemical threats.
- Digitalize, share, and storage X-ray images and other control evidence to improve accuracy of cargo inspections and facilitate criminal investigations.
- Do not deploy screening in sorting centers under the current security landscape and regulatory environment.

As expected, the analysis revealed that collaboration and security culture are important elements of the postal security management. The analysis clarified and juxtaposed interests of key business and government stakeholders in postal security, highlighting critical conflicts that may deadlock future progress of the postal security management. Certain solutions were found to incentivize and align interests of key stakeholders. To strengthen the security culture, Swiss Post might need to revise its human resource management practices. Increasing remuneration for the lowest paid staff segment and security-related bonuses and incentives might bring security benefits through lower staff turnover, more skilled personnel, and more committed and motivated people. Lower dependency on outsourced and temporal workforce would likely to increase security culture further and make it more difficult for criminals and terrorists to infiltrate the Swiss Post's organization. The analysis found that the current regulatory control over postal security management seems justified and proportional to the threats the postal service faces today in Switzerland. We observed that given the criticality of the postal service to the Swiss economy and the society, the Swiss civil protection authorities, might need to consider regulating Swiss Post to ensure that Swiss Post could continue its operations under national, regional, or global emergencies. We found also that the postal industry would benefit from a suite of (voluntary) best practices for preventing and investigating mail theft. Otherwise, rather than imposing more stringent regulations, or start regulating postal security beyond

customs and aviation security areas, the future regulatory focus should be on enforcing postal operator's compliance with the existing rules. At a global level, in particular, the UPU should establish an independent office of validators to audit postal operators' compliance with the two mandatory postal security standards (S58 & S59). The auditing system would be ideally performance-based, it would be built on common auditing criteria, and there would be a possibility of an unannounced audit. Lastly, whenever needs for further regulation arise, it is crucial that the postal industry communicates with regulators and policy makers with one voice, through UPU or other international organizations. The main tenets for collaboration and culture are the following:

- Consider raising salaries of the lowest earning staff segments to attract and retain quality work force and make people more committed to organization's security culture.
- Reconsider use of outsourced and temporal workforce, especially in high-security facilities / functions. Less external workers imply fewer opportunities for criminals and terrorists to infiltrate into an organization.
- Compile a best practice guidebook for countering mail theft
- Do not regulate postal security beyond the customs security and the aviation security domains. Instead of introducing new regulations, focus on compliance monitoring.
- Continue speaking with one voice through the UPU or other central organizational, making sure that regulators understand the special character of the postal service.
- Specify AEO-S requirements for postal operators before the requirements of the new Union Customs Code become applicable.

Summary

This chapter applied the model of logistics-friendly supply chain security management to the case study on the Swiss-centric cross-border postal logistics network. This analytical exercise revealed a set of promising concepts that could be used to improve postal security management in Switzerland and potentially elsewhere. In particular, the analysis suggested that emphasis of future postal security management efforts should focus especially on compliance monitoring of existing standards and regulations (rather than introducing new rules), security-centric human resource management, building capabilities to cope with security-induced uncertainty, and sharing of security control evidence and intelligence.

Chapter 7 | Conclusions

This final chapter opens with a brief summary of the main research findings, conclusions, and recommendations of this PhD project. The chapter proceeds to discuss how the findings contribute to the theory and practice of supply chain security management. The following section reflects generalizability of the findings and the recommendations beyond the study's immediate research context. Concluding the whole thesis, the chapter highlights key topic areas and methodological considerations for future supply chain security research.

7.1. Summary of findings

This section sums up key findings of this PhD project. In chapter 4, we identified and characterized risks that the SCS management addresses and captured them under a unified theoretical frame – the supply chain crime taxonomy. The taxonomy study reveals that supply chain security risks stem from intentional criminal activities. We also found that the commercial supply chains are threatened by a large variety of crime problems, ranging from document fraud to illegal immigration and from counterfeiting to terrorism. The managers were particularly anxious about the risk of terrorism, cyber crime, and cargo theft. Other important managerial concerns included the possibility of criminals masking their illegal activities behind front companies or using insider information to circumvent security systems. But despite the variety, we observed that criminals interact with the supply chain three main ways: 1) they take assets out of the supply chain, 2) they insert contraband or weapons into the supply chain, and 3) they attack directly the supply chain. In addition to the three main ways of criminal interaction, the criminals often facilitate their activities with means and methods, which are not directly connected with the supply chain. Together these observations allowed us to define four crime classes of the supply chain crime taxonomy: *theft*, *smuggling*, *direct attack*, and *facilitating crime*. The taxonomy shows how the criminals both victimize the supply chain (e.g., theft of and damage on cargo) and exploit it as vehicle for crime and destruction (e.g., smuggling illegal drugs and letter bombs). Moreover, the taxonomy illustrates how the global supply chains are closely connected to many transnational criminal phenomena, most notably terrorism, counterfeiting, and drug trafficking. Further elaboration showed that crimes in different taxonomic classes trigger supply chain disruptions of differing levels of magnitude and attract varying amount of government and business interest. We also found out that crimes in the *theft*

and *smuggling* classes involve cargo tampering, thus suggesting that supply chain integrity – defined as the freedom of the supply chain from criminal exploitation – is an important concept in supply chain security risk mitigation.

The findings of the literature synthesis (Ch. 3) imply that the extant SCS discipline is more empirically grounded and diverse than the previous literature reviews suggest. We learned that the SCS discipline has attracted cross-disciplinary and steadily growing academic interest since 2001, and that the SCS research has undergone a shift from conceptual studies towards empirical and analytical investigations. Leading themes in the SCS literature are the screening of shipping containers, protection of cargo from theft and tampering, building security culture, and the selection of a optiomal mix of security solutions among multiple alternatives. The synthesis suggests that SCS solutions cover a wide range of technological devices, procedures, and management principles, and that these solutions are often implemented in combinations rather than separately. The academic community somewhat agrees that the performance of the SCS solutions is defined in terms of their ability to prevent, detect, and help recover from crime. Still, difficulties in obtaining quality data make measurement of the SCS performance rather challenging. The synthesis also suggested that although there are no universal optimal rules for the SCS management, certain design principles exist, and these principles should be considered when SCS management decisions are made. The key principles concern the selection of the SCS solutions, capacity and intensity of the security solutions, integration of the solutions into the sequence of baseline logistics activities, secrecy of information, and the collaboration and culture. The key message of these principles is that the SCS management is as much a question about what to implement as it is about how, where, and to what degree to implement.

The case study chapter described the international postal service from the Swiss perspective, putting a special emphasis on SCS management and law enforcement. The case description reveals that there are nine main domains of postal security management, each aiming at their distinctive goals and fostering a different set of SCS solutions. Different domains target different threats and segments of the postal traffic. Also frequency, intensity, and range of applied security solutions vary across the security domains. The airmail traffic is far the most secured segment of the international postal traffic, owing to the relatively stringent aviation security regulations that impose screening for 100% of the airmail items and sometimes even rescreening of transferring / transiting traffic. However, the airmail security screening target only airmail security threats – explosive and incendiary devices. Other types of security threats (biological, chemical, and radioactive) and contraband in general are controlled mostly in border controls when postal items are exported, imported, or conveyed through transit countries. Though the border controls target basically all security threats and contraband types, the number and the stringency of the existing border controls seem low, though proportional to the current terrorist and crime threats. Certainly border control agencies collect and analyze

traffic information systematically to risk profile incoming shipments and target controls according to their risk levels. But physical examination of cross-border postal items occurs rarely, especially in case of exports and transit traffic. Interestingly, as soon as postal items enter the Swiss national postal system, they are no longer subject to any additional controls, except for highly exceptional police operations or mailroom security procedures at recipients' premises.

Application of the design principles into the case study context identified a set of promising concepts for improving the postal security management. Future postal security management should mainly focus on compliance monitoring of existing regulations rather than creating new ones. The compliance monitoring is particularly important to oversee whether postal operators worldwide comply with the requirements of the two UPU's security standards (S58 and S59). In general, there is no need to start regulating postal security beyond airmail security and customs security areas. The postal industry might anyhow benefit from following regulatory and standardization activities: compilation of a best practice guidebook for addressing mail theft, revision of critical infrastructure regulations in the postal context, and formal specification of post-specific criteria for applying the AEO-S status. The case analysis also highlights the Swiss Post's need to reconsider compensation, hiring, and training policies from the security perspective. The findings of the case analysis also suggests that Swiss Post and Swiss authorities should increase their preparedness to deal with security contingencies: new threats, heightened security requirements, or crime-triggered disruptions of the postal service. Ways to building the preparedness include maintenance of redundant and/or flexible security resources include cross-training of employees, modular design of security systems, and setting up of mobile security teams. The analysis also proposed new modes of collaboration worth pursuing, such as the digitalization and sharing of security control evidence.

7.2. Implications to theory

Certain findings of this dissertation contribute to the theory building in the SCS discipline. The supply chain crime taxonomy captures supply chain crime under a unifying theoretical frame. It strengthens further the ontological basis of the SCS discipline by identifying, characterising, and categoring risks that SCS management addresses. Much of the academic value of the taxonomy research lies in its conceptual refinement. Security risk, for example, is a notoriously ambiguous concept that bears diverse meanings and connotations in various contexts. By defining the character of security risk, the taxonomy clarifies and bridges the gap between the SCS lexicons academics, managers, and authorities are using today. The taxonomy also highlights a distinction between risk sources and risk consequences. Whereas security risk sources represent only a special sub-set of all supply chain hazards (risks arising from man-made, intentional, criminal activities), consequences of security risks are multifaceted and often transcend far beyond the business and supply chain context. This distinction justifies the

position of the academic SCS research as a standalone discipline rather than a sub-field of the general supply chain risk management (SCRM). The distinct character of the security risk also invites the academic community to develop theories and conduct research that fit the particular needs of security risk mitigation. As security risks arise from intentional man-made activities, research in preventive and investigative supply chain security should be rooted in criminological theories, which have investigated psychological aspects of criminal reasoning for centuries.

One of the fiercest debates in the SCS discipline has been the effect of SCS implementation on the SCS performance and logistics performance (e.g., Lee and Whang 2005; Gutiérrez 2007). Scholars on the both side of the debate present plausible arguments and display convincing data. However, the problem is that no one has synthetized this evidence so far. The literature synthesis did exactly this: it collected pieces of academic arguments and empirical evidence and arranged them into a unified framework – the model of logistics-friendly SCS management. The literature synthesis produced also a research agenda that shows the way for original studies with high academic impact.

The case study produced mainly results that are more relevant for practice than for the theory. Nevertheless, the case study description enabled us to test validity of the supply chain crime taxonomy and applicability of the model of logistics-friendly SCS. Reflection of the two frameworks against the empirical reality lent support to the validity of these academic constructs.

7.3. Contribution to practice

Some results of this PhD project have important practional implications. The supply chain crime taxonomy provides a new perspective on the practice of the SCS management. It shows how global supply chains are closely associated with many transnational criminal phenomena, including drug trafficking, nuclear proliferation, counterfeiting, and cyber crime. The intimate association between the transnational crime and the supply chain suggests that one can fight many global crime problems simultaneosly through the SCS management. This is a key insight for international law enforcement agencies such as INTERPOL and EUROPOL that coordinate police cooperation against the whole spectrum of transboundary crimes. These law enforcement agencies as well as WCO should start considering the global supply chain as a key enabler of cross-border criminal operations and the SCS management as a means to fight seemingly unconnected criminal phenomena simultaneously and effectively. The taxonomy also reveals three primary ways how criminals interact with the supply chain: 1) by taking assets out of the supply chain, 2) by introducing unauthorized goods into the supply chain, and 3) by directly attacking the supply chain. This insight allows help practitioners design cost-effective solutions

that reduce crime opportunities, discourage potential offenders, protect supply chain integrity, detect and intercept crime, and facilitate criminal investigations.

The literature synthesis reveals a set of principles, which seem to underpin logistics-friendly design of SCS management, and arranges these design principles into a model. Thanks to this model, real-world decision makers can easily confirm whether they have considered all design principles that the academic SCS literature considers important. The second outcome of the literature synthesis, the research agenda, would make a practical contribution if academics followed the proposed lines of future research, managed to find meaningful results, and succeeded to communicate the results to the practitioners.

The case analysis generated promising evidence-based concepts for improving the postal security management in Switzerland and elsewhere. Adopting these concepts would likely make the international postal logistics faster and more predictable and thus help the postal operators to compete with the express couriers and capitalize on the rapidly growing international e-commerce market. Moreover, the adoption of these concepts is a cost-efficient way to improve performance of the postal security management – the ability to prevent, detect, intercept, and investigate crime and terrorism. Generally, the case description allows Swiss Post and Swiss authorities to rethink their approaches to the postal security. It also gives foreign postal operators and authorities a unique opportunity to benchmark their activities against the Swiss approach. The case study findings also contribute to the ongoing discussion on optimal ways for securing the international postal traffic. In particular, the case study findings contribute to implementation of many EU-level policies, most notably the Customs 2020 and the Integrated e-Commerce programs. The analysis on the airmail security might support and inspire working groups to finalize the Union Customs Code, a regulatory frame that seeks, among other objectives, reform the customs and security management in the postal sector-

7.4. Generalizability of findings

The earlier sections might have convinced you that the findings of this study could have some important implications to the theory and the practice of the SCS management. Now the key question is whether and to what extent these findings and implications apply beyond the study's immediate context. To shed light on this question, the following paragraphs discuss the generalizability of the research findings.

In case of the supply chain crime taxonomy, the managerial descriptions allowed us to understand what cargo owners (shippers and consignees) and logistics service providers (e.g., carriers, freight forwarders, and customs brokers) are thinking about crime in the supply chain context. However, because the research focused exclusively on the managerial thinking, it overlooked the views of customs, police, transport and other authorities, that play a key role in securing the supply chain from crime. The managerial focus raises concerns whether the

taxonomy omits some consequential taxonomic crime classes or defines the current four classes inaccurately, thus providing a distorted picture of the overall supply chain crime phenomenon. Fortunately, the validation of the taxonomy with the case study evidence, which involves also perspectives of the Swiss customs and police authorities, alleviate these concerns to some extent. Indeed, the case validation did lend its support to the taxonomy's applicability in the postal logistics context: no case study evidence implied need for additional taxonomic classes or major revisions of the current ones. Altogether, given the diverse sample of managers who provided their invaluable inputs to this study and the support of the case study validation, we can be fairly confident that the taxonomy captures essential supply chain crime problems across industries[114]. However, I invite scholars and practitioners to further debate and test the taxonomy.

The systematic literature review has one major limitation when it comes to the generalizability. The review focused on peer-reviewed academic studies only, so a large corpus of practitioners' reports, non-published studies, books, and dissertations were left out of the scope. No doubt a great deal of relevant knowledge has been produced outside the peer-reviewed academic publication outlets, and all this knowledge was excluded from the literature synthesis. It is therefore possible that certain important principles of logistics-friendly SCS management did not make it to the model due to the seemingly narrow academic review focus. However, the academic focus left me with a large amount of research to explore, evaluate, and synthetize. After a systematic appraisal of this body of research, I ended up with the final review sample of 41 most relevant and rigorous research articles published on the SCS management after 2001. Owing to the insightful cross-disciplinary, cross-industry, and multi-modal view this sample of articles provides on the SCS management, we can be relatively confident that the model of logistics-friendly SCS management can be applied to address a wide range of SCS design problems.

The single-case research design restricts generalizability of the case study findings and recommendations beyond the Swiss context. There are 192 UPU member countries in the world, and each country has its idiosyncratic political, geographical, economical, social, technological, and legal characteristics. The postal operators themselves differ in terms of the government control, ownership, service portfolio, scope of universal service obligations (USO), and the monopoly power. Therefore, despite the long tradition of standardization in the postal sector, overwhelming contextual differences assure that the Swiss postal service is not precisely similar

[114] The supply chain crime is fundamentally the same across industries, but priorities of different crime problems vary from industry to industry. For instance, pharmaceutical companies are more concerned about theft and product contamination than let say, a company shipping low-value forestry products.

to any other postal service. It should be nevertheless noted that the postal services in the 28 EU countries share important similarities with the Swiss service mainly because of the comparable regulatory environment[115] (see annex A for detailed comparison of the similarities and differences). In addition to the postal operators in the EU countries, also the members[116] of the International Post Corporation (IPC) might consider the case study findings useful and be the first ones to adopt one or more of the recommendations. There might be also some potential for cross-industry generalization. The express courier industry operates somewhat the same way than the postal service, though in a more integrated and faster manner. The express industry also deals with quite the same crime risks than the postal operators: theft, smuggling, and explosives in the air transport channel. This is why express couriers might adopt some of the case study recommendations. Furthermore, the discussion on mail theft prevention and investigation might perhaps interest companies concerned of cargo theft in general, for example the TAPA members.

7.5. Future research

In conclusion of this PhD project, it is worthwhile to take a look on future research needs in the SCS discipline. The literature synthesis (Ch. 3) highlighted some general gaps in the current SCS knowledge. The synthesis concluded that the SCS discipline would benefit from research on air cargo security and cyber crime, two increasingly relevant but so far neglected research themes. It was also found that the extant SCS literature focuses predominantly on management thinking and largely overlooks the viewpoints of government agencies and criminals. Therefore, to broaden the perspective of the SCS knowledge, there is need for more research studying roles of governmental agencies and criminals in the overall SCS management. The synthesis also pointed out that due to a lack of quality data, the past SCS research builds mainly on scarce subjective data and relies on more or less biased proxy measures of the SCS performance. Although it is often difficult to access security-related data, academics should nevertheless try to tap into crime incident statistics, supply chain visibility data, court records and other largely unexploited data sources. Regarding research methods, the literature synthesis highlighted

[115] Recall that Switzerland is integrated in the EU's aviation security regime (OJ L 2002 114/73) and in the EU's customs security regime (OJ L 2009 199, the EU-CH "Agreement on customs facilitation and security"). The former governs airmail security in the EU-28, Switzerland, Norway, and Iceland. The latter governs customs security and set rules for sharing of advance electronic information (AEI), harmonized risk assessment, and the AEO-S program.

[116] The 24 members of the IPC are first world postal operators that are responsible for delivering 80% of the global mail volumes As of September 2014, the members of the IPC are AnPost of Ireland, Australia Post, bpost of Belgium, Canada Post, Correos of Spain, CTT of Portugal, Cyprus Post, Deutsche Post of Germany, Hellenic Post of Greece, Iceland Post, Itella of Finland, La Poste of France, Maguar Posta of Hungary, New Zealand Post, Posten Norge of Norway, Österreichische Post of Austria, Post Danmark of Denmark, Poste Italiane of Italy, Posten AB of Sweden, Post Luxembourg, PostNL of the Netherlands, Royal Mail of the UK, Swiss Post, and the United States Postal Service.

urgency of longitudinal SCS research. The longitudinal research designs would increase our limited understanding of strengths and directions of the cause-effect relationships between SCS implementation, the SCS performance, and logistics performance. Moreover, there is a need to conduct more case-based research to capture subtle contextual nuances that tend to affect substantially outcomes of the SCS implementation.

This PhD project also opens new avenues for future research. The supply chain crime taxonomy invites other researchers to conduct crime type specific studies and to investigate how terrorism, counterfeiting and other overarching crime phenomena are associated with the global supply chain. It would be also interesting to see how governmental agencies perceive crime the supply chain context. The taxonomy itself would benefit from further empirical validation. The two case study chapters set an example for further postal security case studies. It would be great to see analogous case studies being carried in other countries than Switzerland. These additional case studies would allow comparative cross-case analyses, which would likely reveal new insights for the benefit of the postal security management and governance. Moreover, future research could investigate relevant postal security themes that this thesis did not address in detail, for instance money transportation, postal cyber crime, and the postal service as a critical infrastructure.

Finally, this PhD thesis clarified my personal research and professional ambitions. Academically, an interesting follow-up project would be to conduct a security survey with all 192 UPU member states to determine current level of postal security implementation in different countries and regions. Otherwise, I would like to apply my SCS expertise mainly in practice. It would be fascinating to participate in postal security projects, especially if the projects piloted some of the improvement concepts I propose in this thesis. Outside the postal sector, I would like to partake in projects studying theft prevention in the pharmaceutical sectors, use of Big Data in cargo risk profiling, and the role of cyber crime in "off-line" supply chain crime.

Summary

This final chapter summarized research findings of this PhD project and discussed their academic and practical implications. I concluded that the research project consolidates the weak theoretical underpinnings of the SCS discipline: it captures supply chain crime risks under a unifying taxonomy and refines fragments of SCS management knowledge into principles of logistics-friendly SCS design. The application of the design principles in the case study setting produced evidence-based concepts for improving practical postal security management.

However, due to contextual differences, we should be careful when applying the improvement concepts outside Switzerland and in non-postal logistics networks. The chapter concluded by highlighting important topic areas and key methodological considerations for future research.

Bibliography

*References marked with * were analyzed in detail in the systematic literature review (see Annex B).*

Autry, C.W. & Bobbitt, L.M., 2008. Supply chain security orientation: conceptual development and a proposed framework. *The International Journal of Logistics Management*, 19(1), pp.42–64. *

Ayres, I., & Levitt, S. D. (1997). *Measuring positive externalities from unobservable victim precaution: an empirical analysis of Lojack*. National Bureau of Economic Research.

Bailey, K. D. (1994). *Typologies and taxonomies: an introduction to classification techniques*. Sage.

Bakır, N. O. (2011). A Stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research*, *187*(1), 5-22. *

Bakshi, N., & Gans, N. (2010). Securing the containerized supply chain: analysis of government incentives for private investment. *Management Science*, *56*(2), 219-233. *

Bakshi, N., Flynn, S. E., & Gans, N. (2011). Estimating the operational impact of container inspections at international ports. *Management Science*, *57*(1), 1-20. *

Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and justice*, 277-318.

Belzer, M. H., & Swan, P. F. (2011). Supply chain security: agency theory and port drayage drivers. *The Economic and Labour Relations Review*, *22*(1), 41-63. *

Bier, V. M., & Haphuriwat, N. (2011). Analytical method to identify the number of containers to inspect at US ports to deter terrorist attacks. *Annals of Operations Research*, *187*(1), 137-158. *

Boeing, (2012). *World air cargo forecast 2012-2013*.

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). International World Wide Web Conferences Steering Committee.

Clarke, R. V., & Eck, J. (2003). *Become a problem-solving crime analyst: In 55 small steps*. London: Jill Dando Institute of Crime Science University College London.

Closs, D. J., & McGarrell, E. F. (2004). *Enhancing security throughout the supply chain* (pp. 1-52). IBM Center for the Business of Government.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*(4), 933-948.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Incorporated.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.

da Mota Pedrosa, A., Näslund, D., & Jasmand, C. (2012). Logistics case study based research: towards higher quality. *International Journal of Physical Distribution & Logistics Management*, *42*(3), 275-295.

David, P. A., & Stewart, R. D. (2010). *International logistics: the management of international trade operations*. Cengage Learning.

Denyer, D., & Tranfield, D. (2006). Using qualitative research synthesis to build an actionable knowledge base. *Management Decision*, *44*(2), 213-227.

Denyer, D., Tranfield, D., & Van Aken, J. E. (2008). Developing design propositions through research synthesis. *Organization studies*, *29*(3), 393-413.

DG MOVE. (2013). *Transport safety and security in the EU*. Retrieved from http://ec.europa.eu/transport/themes/security/index_en.htm

Dieke, A. K. D., Bender, C., Campbell, J. I., Cohen, R. H., Müller, C., Niederbrüm, A., de Streel, A., & Thiele, S. WIK-Consult GmbH, (2013). *Main developments in the postal sector (2010-2013).*

Diop, A., Hartman, D., & Rexrode, D. (2007). *C-TPAT Cost/Benefit Survey*. Center for Survey Research, University of Virginia.

Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. *Academy of management review*, *32*(4), 1246-1264.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

Ekwall, D. (2009a). *Managing the risk for antagonistic threats against the transport network*. Doctoral dissertation, Chalmers University of Technology.

Ekwall, D. (2009b). The displacement effect in cargo theft. *International Journal of Physical Distribution & Logistics Management*, *39*(1), 47-62. *

Eppler, M. J., Hoffmann, F., & Pfister, R. (2011). *Rigor and relevance in management typologies: Assessing the quality of qualitative classifications*. Working paper.

Erlandson, D. A. (Ed.). (1993). *Doing naturalistic inquiry: A guide to methods*. Sage.

European Alliance for Access to Safe Medicines, (2008). *The counterfeiting superhighway*. Surrey: Medicom Group Ltd.

European Commission , (2010). *Postal service statistics - universal service providers - main figures*. Retrieved from website: http://epp.eurostat.ec.europa.eu/statistics_explained/ index.php/Postal_service_statistics_-_universal_service_providers_-_main_figures.

European Commission, (2012). *Report on EU customs enforcement of intellectual property rights, results at the EU border 2011.*

European Commission, (2014). *Communication on an integrated parcel delivery market for the growth of e-commerce in the EU* (2013/2043(INI).

Eurostat, (2014). *Quality of service*. Retrieved from website: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=post_ps_qs&lang=en.

Eyefortransport, (2011). *Maritime piracy costs global community up to $12 billion a year*. Retrieved from website: http://www.eyefortransport.com/content/ maritime-piracy-costs-global-

community-12-billion-year

Farr, K. A., & Gibbons, D. C. (1990). Observations on the development of crime categories. *International Journal of Offender Therapy and Comparative Criminology*, *34*(3), 223-237.

Field, A. (2009). *Manufacturers say 10 2 costs $20 billion*. Retrieved from J. Commerce Online website: http://www.joc.com/government -regulation/manufacturers-say-102-costs-20-billion

Foddy, W., & Foddy, W. H. (1994). *Constructing questions for interviews and questionnaires: theory and practice in social research*. Cambridge university press.

Frey, J. H., & Fontana, A. (1991). The group interview in social research. *The Social Science Journal*, *28*(2), 175-187.

Gaukler, G. M., Li, C., Ding, Y., & Chirayath, S. S. (2012). Detecting nuclear materials smuggling: Performance evaluation of container inspection policies. *Risk Analysis*, *32*(3), 531-554. *

Glaser, B. G., & Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Grainger, A. (2011). Trade facilitation: a conceptual review. *Journal of World Trade*, *45*(1), 39-62. *

Guba, E. G. (Ed.). (1990). *The paradigm dialog*. Sage Publications.

Gutiérrez, X. (2007). *A Model for the Design of Effective and Resilient Supply Chain Security Management Systems*. Doctoral dissertation, Ecole Polytechnique Fédérale de Lausanne.

Gutierrez, X., & Hintsa, J. (2006, May). Voluntary supply chain security programs: a systematic comparison. *The International Conference on Information Systems, Logistics and Supply Chain, Lyon, France*.

Haelterman, H. (2009). Situational Crime Prevention and Supply Chain Security: An "Ex Ante" Consideration of Preventive Measures. *Journal of Applied Security Research*, *4*(4), 483-500.

Haelterman, H. (2011). Re-thinking the cost of supply chain security. *Crime, law and social change*, *56*(4), 389-405.

Haelterman, H., Callens, M., & Vander Beken, T. (2012). Controlling access to pick-up and delivery vans: the cost of alternative measures. *European Journal on Criminal Policy and Research*, *18*(2), 163-182. *

Hakim, S., & Rengert, G. F. (Eds.). (1981). *Crime spillover*. Beverly Hills, CA: Sage Publications.

Halldórsson, Á., & Aastrup, J. (2003). Quality criteria for qualitative inquiries in logistics. *European Journal of Operational Research*, *144*(2), 321-332.

Hameri, A. P., & Hintsa, J. (2009). Assessing the drivers of change for cross-border supply chains. *International Journal of Physical Distribution & Logistics Management*, *39*(9), 741-761. *

Hintsa, J. (2010). A comprehensive framework for analysis and design of supply chain security standards. *Journal of Transportation Security*, *3*(2), 105-125.

Hintsa, J. (2011). Post-2001 Supply Chain Security—impacts on the private sector. Doctoral dissertation, Université de Lausanne.

Hintsa, J., & Hameri, A. P. (2009). Security programs as part of efficient supply chain management. In *Supply Chain Forum: An International Journal*, *10*(2), 26-37.

Hintsa, J., Ahokas, J., Männistö, T., & Sahlstedt, J. Cross-border Research Association, (2010b). *CEN supply chain security feasibility study*.

Hintsa, J., Gutierrez, X., Wieser, P., & Hameri, A. P. (2009). Supply chain security management: an overview. *International Journal of Logistics Systems and Management*, *5*(3), 344-355.

Hintsa, J., Männistö, T., Hameri, A. P., Thibedeau, C., Sahlstedt, J., Tsikolenko, V., Finger, M. & Granqvist, M. (2011). Customs Risk Management (CRiM): A Survey of 24 WCO Member Administrations. *Cross-Border Research Association*.

Hintsa, J., Männistö, T., Hameri, A. P., Tsikolenko, V., & Schaller, K. (2010a). *Crime and security in postal supply chains*. Trends and innovation for the postal markets conference, Lausanne.

International Civil Aviation Organization / World Customs Organization, (2013). *Air cargo security and facilitation: Moving air cargo globally*.

International Organization for Standardization, (2009). *Risk management vocabulary* (73:2009(E/F))

International Post Corporation / Boston Consulting Group, (2012). *Focus future – building a new compelling position for posts*.

International Post Corporation, (2008). *The natural partner for the postal industry.*

International Post Corporation, (2010). *IPC cross-border e-commerce report.*

International Post Corporation, (2013). *E-commerce and delivery – an IPC strategic perspective.*

International Road Transport Union, (2008). *Attacks on drivers of international heavy goods vehicles: Survey results.*

International Telecommunication Union, (2009). *Measuring the information society, the ICT development index*.

Jaag, C. (2007). Liberalization of the Swiss letter market and the viability of universal service obligations.

Joossens, L., & Raw, M. (2008). Progress in combating cigarette smuggling: controlling the supply chain. *Tobacco control*, *17*(6), 399-404. *

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research and Applications*, *6*(4), 197-210.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and operations management*, *14*(1), 53-68.

Klima, N. (2012). Temporal dimensions of vulnerability to crime in economic sectors: Theory meets evidence and spawns a new framework. *Risk Management*, *14*(2), 93-108. *

Korps landelijke politiediensten, (2009). *National threat assessment 2008: Organised crime.*

Krippendorff, K. (2004). *Content Analysis*. Sage.

Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Sage.

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of production economics*, *96*(3), 289-300. *

Lee, H. L., & Wolfe, M. (2003). Supply chain security without tears. *Supply Chain Management Review*, *7*(3),12-20.

Lee, J., Palekar, U. S., & Qualls, W. (2011). Supply chain efficiency and security: Coordination for collaborative investment in technology. *European Journal of Operational Research*, *210*(3), 568-578. *

Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage.

Männistö, T. (2011), Supply chain security – disclosing user's requirements. Master's thesis, Aalto University School of Science and Technology.

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192-223.

Marine Accident Investigation Branch, (2008). *Report on the investigation of the structural failure of MSC Napoli English channel on 18 January 2007.*

Martens, B. J., Crum, M. R., & Poist, R. F. (2011). Examining antecedents to supply chain security effectiveness: an exploratory study. *Journal of business logistics*, *32*(2), 153-166. *

McCarthy, K. R. C. (2009). *Crime, risk and security in the postal system: the identification and management of risk and security concerns in the'horizontal distribution pipeline'of Royal Mail* (Doctoral dissertation, University of Portsmouth).

McLay, L. A., & Dreiding, R. (2012). Multilevel, threshold-based policies for cargo container security screening systems. *European Journal of Operational Research*, *220*(2), 522-529. *

Meade, C., & Molander, R. C. (2006). Considering the effects of a catastrophic terrorist attack. RAND Corporation, California. *

Merrick, J. R., & McLay, L. A. (2010). Is screening cargo containers for smuggled nuclear threats worthwhile? *Decision Analysis*, *7*(2), 155-171. *

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Morgan, D. L. (1997). *Focus groups as qualitative research*. Sage.

Murray-Tuite, P. M., & Fei, X. (2010). A methodology for assessing transportation network terrorism risk with attacker and defender interactions. *Computer-Aided Civil and Infrastructure Engineering*, *25*(6), 396-410. *

Naim, M. (2006). *Illicit: How smugglers, traffickers and copycats are hijacking the global economy*. Knopf Doubleday Publishing Group.

Naylor, R. T. (2003). Towards a General Theory of Profit-Driven Crimes. *British Journal of Criminology*, *43*(1), 81-101.

Naylor, R. T. (2007). *Marlboro men*. Retrieved from London Review of Books website: http://www.lrb.co.uk/v29/n06/rt-naylor/marlboro-men.

Okholm, H. B., Winiarczyk, M., Moller, A., & Nielsen, C. K. (2010). Main developments in the postal sector (2008-2010). *Copenhagen Economics*.

Organization for Economic Co-operation and Development, (2005). *Container transport security across modes*

Oxford Economics, (2011). *The economic impact of express carriers in Europe*

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Pawson, R., & Tilley, N. (1997). *Realistic evaluation*. Sage.

Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics: Research and Applications*, *9*(2), 127-142.

Pfohl, H. C., Köhler, H., & Thomas, D. (2010). State of the art in supply chain risk management research: empirical and conceptual findings and a roadmap for the implementation in practice. *Logistics Research*, *2*(1), 33-44.

Phillips, D. C., & Burbules, N. C. (2000). *Postpositivism and educational research*. Rowman & Littlefield.

Poyner, B. (1986). A Model for Action. *Situational Crime Prevention–From Theory into Practise*.

PriceWaterhouseCoopers, (2011). *Transportation & logistics 2030 volume 4: Securing the supply chain.*

Prokop, D. (2012). Smart containers and the public goods approach to supply chain security. * *International Journal of Shipping and Transport Logistics*, *4*(2), 124-136.

Reilly, A., Nozick, L., Xu, N., & Jones, D. (2012). Game theory-based identification of facility use * restrictions for the movement of hazardous materials under terrorist threat. *Transportation research part E: logistics and transportation review*, *48*(1), 115-131.

Repenning, N. P., & Sterman, J. D. (2001). Nobody ever gets credit for fixing problems that never happened. *California management review*, *43*(4), 64-88.

Rice, J. B., & Caniato, F. (2003). Building a secure and resilient supply network. *Supply chain management review*, *7*(5), 22-30.

Rice, J. B., & Spayd, P. W. IBM, Center for Business Government. (2005). *Investing in supply chain security: Collateral benefits.*

Roach, J. A. (2004). Initiatives to enhance maritime security at sea. *Marine Policy*, *28*(1), 41-66. *

Rousseau, D. M., Manning, J., & Denyer, D. (2008). 11 Evidence in Management and Organizational Science: Assembling the Field's Full Weight of Scientific Knowledge Through Syntheses. *The academy of management annals*, *2*(1), 475-515.

Russell, D. M., & Saldanha, J. P. (2003). Five tenets of security-aware logistics and supply chain * operation. *Transportation Journal*, 44-54.

Sarathy, R. (2006). Security and the global supply chain. *Transportation journal*, 28-51.

Seuring, S., & Gold, S. (2012). Conducting content-analysis based literature reviews in supply chain management. *Supply Chain Management: An International Journal*, *17*(5), 544-555.

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *International Journal of Logistics Management*, *12*(2), 1-11.

Sheffi, Y. (2005). The resilient enterprise: overcoming vulnerability for competitive advantage. *MIT Press Books*, *1*.

Sheu, C., Lee, L., & Niehoff, B. (2006). A voluntary logistics security program and international * supply chain partnership. *Supply chain management: an international journal*, *11*(4), 363-374.

Signoret, J. E. (2009). On Cargo Security Measures and Trade Costs. *Global Economy Journal*, * *11*(3), 2-23.

Simatupang, T. M., Wright, A. C., & Sridharan, R. (2002). The knowledge of coordination for supply chain integration. *Business process management journal*, *8*(3), 289-308.

Sodhi, M. S., Son, B. G., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management*, *21*(1), 1-13.

Sowerby, B. D., & Tickner, J. R. (2007). Recent advances in fast neutron radiography for cargo

inspection. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, *580*(1), 799-802.

Speier, C., Whipple, J. M., Closs, D. J., & Voss, M. D. (2011). Global supply chain design considerations: mitigating product safety and security risks. *Journal of Operations Management*, *29*(7), 721-736. *

Staake, T., Thiesse, F., & Fleisch, E. (2009). The emergence of counterfeit trade: a literature review. *European Journal of Marketing*, *43*(3/4), 320-349. *

Sternberg, H., Nyquist, C., & Nilsson, F. (2012). Enhancing Security Through Efficiency Focus—Insights From a Multiple Stakeholder Pilot Implementation. *Journal of Business Logistics*, *33*(1), 64-73. *

Swiss Post, (2010). *Annual report 2010.*

Swiss Post, (2011). *We move people, goods, money and information in a reliable, value enhancing and sustainable way.*

SwissMedic, (2013). *Fewer illegal imports of medicinal products*. Retrieved from website: https://www.swissmedic.ch/aktuell/00673/01441/index.html?lang=en

Talas, R., & Menachof, D. A. (2009). The efficient trade-off between security and cost for sea ports: a conceptual model. *International journal of risk assessment and management*, *13*(1), 46-59. *

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British journal of management*, *14*(3), 207-222.

Transparency International, (2012). *Corruption perceptions index 2012.*

United Nations Office on Drugs and Crime (2010). *The globalization of crime: A transnational organized crime threat assessment*. United Nations Publications.

United Nations Office on Drugs and Crime (2011). *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes*. United Nations Publications.

Universal Postal Union, (2012). *Postal statistics – a summary, economic and regulatory affairs directorate.*

Urciuoli, L. (2010). Supply chain security—mitigation measures and a logistics multi-layered framework. *Journal of transportation security*, *3*(1), 1-28.

Urciuoli, L. (2011). Investing in transport security solutions: using the quantitative risk assessment (QRA) approach. *International Journal of Risk Assessment and Management*, *15*(4), 275-298. *

Urciuoli, L., Männistö, T., Khan, T., & Hintsa, J. (2013). Supply chain cyber security: Potential threats. *Information & Security: An International Journal*, *29*(1), 51-68.

van den Engel, A. W., & Prummel, (2007). *Organised theft of commercial vehicles and their loads in the European Union* (PE 379.229)

Van Weele, S. F., & Ramirez-Marquez, J. E. (2011). Optimization of container inspection strategy via a genetic algorithm. *Annals of Operations Research*, *187*(1), 229-247. *

Voss, M. D., Whipple, J. M., & Closs, D. J. (2009a). The role of strategic security: internal and external security measures with security performance implications. *Transportation Journal*, *48*(2), 5-23. *

Voss, M. D., Closs, D. J., Calantone, R. J., Helferich, O. K., & Speier, C. (2009b). The role of security in the food supplier selection decision. *Journal of Business Logistics*, *30*(1), 127-155. *

Waters, C. D. J. (2003). *Logistics: an introduction to supply chain management*. New York City: Palgrave Macmillan.

Wein, L. M., Wilkins, A. H., Baveja, M., & Flynn, S. E. (2006). Preventing the importation of illicit nuclear materials in shipping containers. *Risk Analysis*, *26*(5), 1377-1393. *

Whipple, J. M., Voss, M. D., & Closs, D. J. (2009). Supply chain security practices in the food industry: Do firms operating globally and domestically differ?. *International Journal of Physical Distribution & Logistics Management*, *39*(7), 574-594. *

Widdowson, D. (2005). Managing risk in the customs context. *Customs Modernization Handbook*, 91-99. World Bank Publications.

Williams, Z., Lueg, J. E., Taylor, R. D., & Cook, R. L. (2009a). Why all the changes?: An institutional theory approach to exploring the drivers of supply chain security (SCS). *International Journal of Physical Distribution & Logistics Management*, *39*(7), 595-618. *

Williams, Z., Lueg, J.E. & LeMay, S.A., (2008). Supply chain security: an overview and research agenda. The International Journal of Logistics Management, 19(2), pp.254–281. *

Williams, Z., Ponder, N. & Autry, C.W., (2009b). Supply chain security culture: measure development and validation. The International Journal of Logistics Management, 20(2), pp.243–260. *

World Bank, 2012. *Connecting to compete: Trade logistics in the global economy.*

World Economic Forum, (2012). *Illicit trade: issue overview*. Retrieved from World Economic Forum website: https://members.weforum.org/pdf/GAC09/council/illicit_trade/

Yang, C. C., & Wei, H. H. (2013). The effect of supply chain security management on security performance in container shipping operations. *Supply Chain Management: An International Journal*, *18*(1), 74-85. *

Yang, Z. L., Wang, J., Bonsall, S., & Fang, Q. G. (2009). Use of fuzzy evidential reasoning in maritime security assessment. *Risk Analysis*, *29*(1), 95-120. *

Yin, R.K., (2009). Case Study Research, Sage Publications.

Annex A | Comparison of postal operators

Tables in the following pages illustrate key differences between postal services in Europe. The bullet points below describe main data sources I used to compile the tables:

- "The Transparency int'l score" comes from the corruption perceptions index 2012 of the Transparency International.

- "The LPI customs indicator" corresponds the "border procedures and time" component of the World Bank's logistics performance indicator that was published in the report "Connecting to compete: Trade logistics in the global economy" in 2012.

- The "on-time delivery performance of international first-class letters" measure comes from the Eurostat database (European Commission 2010).

- The ICT development index is taken from the report "Measuring the information society, the ICT development index 2009" of the International Telecommunication Union.

							Ownership			Monopoly						
Country		Rank	EU member	IPC member	GDP / capita (thousand US$) 2012	Total volume (million)	State	Mixed	Private	None	Restricted	Transparency int'l score	LPI customs indicator	On-time delivery performance of 1st class letters 2010	ICT development index 2011	Score
Denmark	DK	1	1	1	56	890	1	0	0	1	0	90	3,93	93,3	8,29	3,9
Finland	FI	2	1	1	46	1609	1	0	0	1	0	90	3,98	91,1	8,04	3,8
Sweden	SE	3	1	1	55	2869	1	0	0	1	0	88	3,68	93,7	8,34	3,8
Switzerland	**CH**	4	**0**	**1**	**79**	**3752**	**1**	**0**	**0**	**0**	**1**	**86**	**3,88**	**97,2**	**7,68**	**3,8**
Netherlands	NL	5	1	1	46	4670	0	0	1	1	0	84	3,85	95,2	7,82	3,7
Luxembourg	LU	6	1	1	107	187	1	0	0	1	0	80	3,54	98,0	7,76	3,6
Germany	DE	7	1	1	42	20229	0	1	0	1	0	79	3,87	94,0	7,39	3,6
Iceland	IS	8	0	1	43	38	1	0	0	0	1	82	3,53	87	8,17	3,6
United Kingdom	GB	9	1	1	39	18518	1	0	0	1	0	74	3,73	87,9	7,75	3,5
Belgium	BE	10	1	1	43	2586	0	1	0	1	0	75	3,85	93,3	6,89	3,5
Norway	NO	11	0	1	100	1410	1	0	0	0	1	85	3,46	85,1	7,52	3,5
Austria	AT	12	1	1	47	2967	0	1	0	1	0	69	3,77	95,4	7,1	3,5
France	FR	13	1	1	40	17148	1	0	0	1	0	71	3,64	83,4	7,3	3,4
Ireland	IE	14	1	1	46	681	1	0	0	1	0	69	3,4	85,0	7,09	3,3
Slovenia	SI	15	1	0	22	344	1	0	0	1	0	61	3,05	95,5	6,7	3,2
Portugal	PT	16	1	1	20	1061	1	0	0	1	0	63	3,19	94,7	6,05	3,1
Malta	MT	17	1	0	21	38	0	1	0	1	0	57	2,81	95,3	6,69	3,1
Estonia	EE	18	1	0	16	78	1	0	0	1	0	64	2,51	92,7	6,81	3,0
Cyprus	CY	19	1	1	26	95	1	0	0	0	1	66	3,02	90,0	5,73	3,0

							Ownership			Monopoly						
Country		Rank	EU member	IPC member	GDP / capita (thousand US$) 2012	Total volume (million)	State	Mixed	Private	None	Restricted	Transparency int'l score	LPI customs indicator	On-time delivery performance of 1st class letters 2010	ICT development index 2011	Score
Czech Rebublic	CZ	20	1	0	19	861	1	0	0	1	0	49	2,95	93,2	6,17	2,9
Italy	IT	21	1	1	33	4750	1	0	0	1	0	42	3,34	88,6	6,28	2,9
Hungary	HU	22	1	1	13	891	1	0	0	1	0	55	2,82	93,7	5,77	2,9
Latvia	LV	23	1	0	14	42	1	0	0	1	0	49	2,71	97,3	6,06	2,9
Slovakia	SK	24	1	0	17	335	1	0	0	1	0	46	2,88	96,8	5,86	2,9
Croatia	HR	25	1	0	13	305	1	0	0	1	0	46	3,06	86,9	5,75	2,8
Poland	PL	26	1	0	13	2002	1	0	0	1	0	58	3,3	**53,4**	6,19	2,7
Bulgaria	BG	27	1	0	7	234	1	0	0	1	0	41	2,97	**83,6**	5,24	2,6
Lithuania	LT	28	1	0	14	81	1	0	0	1	0	54	2,73	**65,0**	6,06	2,6
Greece	GR	29	1	1	22	542	0	1	0	1	0	36	2,38	**87,7**	6,14	2,6
Spain	ES	30	1	1	29	4943	1	0	0	1	0	65	3,4		6,62	2,3
Romania	RO	31	1	0	8	511	0	1	0	1	0	44	2,65	52,6	5,13	2,3
Median / %			90 %	65%	29	890,4	77 %	19 %	3 %	87 %	13 %	65	3,34	93,0	6,7	3,1
Max					107	20229						90	3,98	98,00	8,34	3,85
Min					7	38						36	2,38	52,60	5,13	2,27
CH RANK					**3**	**7**						**4**	**3**	**3**	**8**	**4**
TOTAL			28	20	1096	94668	24	6	1	27	4					

Annex B | Data extraction forms

This annex presents complete data extractions forms of the 41 reviewed articles that I analyzed in the systematic literature review in chapter 3. The template shell of the data extraction form is displayed in table right below.

Category	Data field	Data field
Overview	Problem statement	1.1.
	Objective of the study	1.2.
	Type of paper	1.3.
	Approach and methods	1.4.
Context	Settings	2.1.
	Focal crime or security risk	2.2.
Intervention	What security solutions are studied?	3.1.
Mechanism	What contextual factors activate the solution-outcome association?	4.1.
	What contextual factors influence the solution-outcome association?	4.2.
Outcome	What are observed / assumed effects of security solutions?	5.1.

The actual article-specific data extraction forms are the following:

Autry and Bobbit 2008

Supply chain security orientation: conceptual development and a proposed framework

Data field	
1.1.	Even though SCS has become increasingly important managerial domain, there is little understanding what security aware firms are, what enables and drives security awareness, and what are the outcomes of 'supply chain security orientation'.
1.2.	To conceptualize, validate, operationalize, and theorize on the construct of SCS orientation.
1.3.	Empirical
1.4.	Interviews (31), cross-sectional
2.1.	US-based companies.
2.2.	N/A
3.1.	SCS orientation consisting of security preparation and planning, security-related partnerships, organizational adaptation and security-dedicated communications and technology
4.1.	Potential antecedents: security vulnerabilities, risk perceptions, and partner directive.
4.2.	Potential moderators:

	Internal: Top management support, employee security attitudes, and employee integrity/loyalty External: Political/legal factors/support, partner cooperation, and partner support
5.1.	Potential outcomes: performance at firm, operational and market levels, customer satisfaction and supply chain continuity

Bakir 2011

A Stackelberg game model for resource allocation in cargo container security, Annals of Operations Research

Data field	
1.1.	Terrorists, who may smuggle weapons of mass destruction (WMD) into the US, are adaptable adversaries. Authorities face a challenge when they try to allocate scarce security-related resources cost-effectively across technologies and locations.
1.2.	To analyze resource allocation strategies against an adaptive adversary to secure cargo container transportation.
1.3.	Analytical
1.4.	Game-theoretical modeling with the Stackelberg's game where defenders (US authorities act first and attackers (terrorists) after.
2.1.	US-bound sea container traffic
2.2.	Smuggling of weapons in sea containers
3.1.	Resource allocation across physical security, in-box sensor technology, non-intrusive inspection in domestic and foreign ports.
4.1.	Uneven security levels at different sites along the supply chain make the most vulnerable spot attractive targets for terrorists.
4.2.	Terrorists' capability to detonate WMDs remotely decrease effectiveness of domestic port security solutions.
5.1.	Cost and delays and increased ability to detect and foil an attack.

Bakshi and Gans 2010

Securing the containerized supply chain: Analysis of government incentives for private investment, Management Science

Data field	
1.1.	Terrorist may use container traffic to smuggle weapons of mass destruction into the US. Business-private partnership programs like C-TPAT are promising ways to reduce cost and delays associated with security controls. However, there is not much information how trading companies could be incentivized to join the C-TPAT programs and what would be consequences of different incentives on the terrorist threat.
1.2.	To understand economic tradeoffs embedded in container inspection decisions and analyze related policy options.

1.3.	Analytical
1.4.	Game-theoretical modeling with the sequential Stackelberg's game where CBP, trading firms and terrorists make their decisions in turns.
2.1.	US-bound sea container traffic
2.2.	Smuggling of weapons of mass destruction into the US.
3.1.	The C-TPAT program
4.1.	N/A
4.2.	(Strategic) delays for inspecting containers of non-C-TPAT certified companies could increase the number of C-TPAT members.
5.1.	Costs for CBP (US Customs and Border Protection) and trading firms. Risk of terrorist smuggling weapons of mass destruction into the US.

Bakshi et al. 2011

Estimating the Operational Impact of Container Inspections at International Ports, Management science

Data field	
1.1.	The US government is pushing a new 100 % screening mandate for US-bound containers in foreign ports. The 100 % regime is a major concern for foreign port operators because the current CSI regime seems not to be scalable for high inspection rates.
1.2.	To simulate impacts of two container inspection regimes in terms of port congestion, handling cost and dwell time.
1.3.	Empirical
1.4.	Discrete event queuing network simulation with real container movement data from two of the world's busiest container terminals.
2.1.	US-bound container traffic in oversea ports.
2.2.	Smuggling of weapons of mass destruction into the US.
3.1.	The CSI programs and its variations.
4.1.	N/A
4.2.	Changes in the positions of inspection spots and rules how containers are selected for inspection.
5.1.	Handling cost, congestion, dwell time and inspection rate.

Belzer and Swan 2011

Supply Chain Security: Agency Theory and Port Dryage Drivers, The Economic and Labour Relations Review

Data field	
1.1.	Owner-operator dryage drivers (short distance haulers of intermodal containers) are among the lowest compensated employees in the USA. Low pay may lead to low security and provide

	terrorists a relatively easy access to containers.
1.2.	To discuss supply chain security from the perspective of behavioral economics, labor market issues and industrial relations.
1.3.	Review
1.4.	Interpretation of survey data and statistics
2.1.	US seaports. The authors discuss both inbound and outbound container traffic.
2.2.	Use of sea containers in terrorist attacks or as means to support terrorist activities.
3.1.	"Efficiency wages" (i.e., salary above market clearing prices), increased supplier/worker monitoring and program for background checks.
4.1.	N/A
4.2.	* Low compensation results in lower quality work force and poor security. This is because few people are willing to accept and stay in the job if there are any other available options. * Short distance dryage hauliers are ubiquitous and thus difficult, if not impossible, to control. * Efficiency wage would help attract and retain competent and reliable people as well as make these people more vigilant for security threats. The drivers would be afraid that security breaches would result in layouts and they would lose their efficiency wages.
5.1.	Lower risk that terrorist get their hands on container traffic.

Bier and Haphuriwath 2011

Analytical Method to Identify the Number of Containers to Inspect at U.S. Ports to Deter Terrorist Attacks, Annals of Operations Research

Data field	
1.1.	Terrorist may smuggle weapons into the US in containers. There is not consensus whether a certain inspection strategy would deter terrorists from attempting the attack altogether.
1.2.	To determine how many containers would need to be screened in order to deter smuggling attempts.
1.3.	Analytical
1.4.	Game-theoretical modeling
2.1.	US-bound sea container traffic
2.2.	Smuggling of weapons into the US, especially nuclear devices and radiological material.
3.1.	Proportion of containers screened as part of maritime security programs. Credibility of defenders retaliation.
4.1.	N/A
4.2.	* Credible threat of retaliation discourages terrorists from attempting an attack. * Sufficiently high risk of getting detected may deter terrorists from attempting to smuggle nuclear devices and radioactive material to the US. Attackers could be deterred by inspecting less than 100 % of containers. * Cost of smuggling attempt influences the threshold when terrorist are deterred to attempt smuggling. For instance, in case of relatively low value conventional weapons like assault rifles, smugglers tolerate higher likelihoods of getting detected. If this premise holds, then the most expensive attacks for terrorists, that are often also the most devastating ones for the defenders, are most easily deterred.

	* Deterrence may simply deflect (or displace) attacks to locations of lower defenses. Or terrorists may change their modus operandi.
5.1.	Higher capability to detect and deter smuggling attempts.

Ekwall 2009b

The displacement effect in cargo theft, International Journal of Physical Distribution and Logistics Management

Data field	
1.1.	Cargo theft has always been a problem for shippers and logistics service providers. Regardless of the persistent efforts to reduce cargo theft, crime continues to strive.
1.2.	To analyze and explain why cargo theft continues to occur in the transport network despite all implemented countersolutions
1.3.	Empirical
1.4.	Interviews with six subject matter experts (cross-sectional), survey with four terminal operators (cross-sectional), and macro-statistics from TAPA (Transported Asset Protection Association)
2.1.	Focus is on Swedish transport networks and logistics facilities.
2.2.	Cargo theft
3.1.	N/A
4.1.	Change in security level in one location in a transportation network.
4.2.	N/A
5.1.	* Some evidence on crime displacement in terms of method (modus operandi). Cargo thieves target increasingly cargo in-transit because logistics facilities are nowadays better protected. * Displacement is likely to be partial in contrast to complete displacement. This means that absolute crime theft risk can be reduced.

Gaukler et al. 2012

Detecting Nuclear Materials Smuggling: Performance Evaluation of Container Inspection Policies, Risk Analysis

Data field	
1.1.	Current ATS-based (Automated Targeting System) inspection policy might be suboptimal strategy when trying to detect well-shielded nuclear material in US-bound containers.
1.2.	To demonstrate weaknesses of container inspection policy and propose more effective alternative approaches.
1.3.	Analytical
1.4.	Queuing network modeling
2.1.	US-bound container traffic
2.2.	Smuggling of well-shielded nuclear material into the US.

3.1.	Passive radiation sensors, ATS, and container-type specific adjustment of sensor alarm thresholds.
4.1.	Reliability of intelligence and allowable inspection delay determine the optimal inspection policy.
4.2.	* Type of information collected with inspection technologies, thresholds of sensors and decision rules applied over the inspection process influence detection probability and delays. * Container type specific thresholds reduce rate of false alarms and reduce consequently delays and costs.
5.1.	Trade-off between detection probability and delays.

Grainger 2009

Trade Facilitation: A Conceptual Review, Journal of World Trade

Data field	
1.1.	Trade facilitation is an increasingly important topic when considering expanding international trade and increased requirements for supply chain security.
1.2.	To provide conceptual overview on trade facilitation by outlining its scope, goals, elements and principles.
1.3.	Review
1.4.	Review of policy documents, previous literature and regulations.
2.1.	Global trade
2.2.	N/A
3.1.	SCS initiatives that may hinder international trade
4.1.	N/A
4.2.	SCS may become a non-tariff barrier for trade.
5.1.	N/A

Haelterman et al. 2012

Controlling Access to Pick-up and Delivery Vans: The Cost of Alternative Solutions, European Journal on Criminal Policy and Research

Data field	
1.1.	The situational crime prevention theory suggests that preventive security solutions may easily backfire. However, many managers do not have a holistic picture which kind of considerations should precede selection of implementation of security solutions.
1.2.	To demonstrate feasibility of a management model for selecting preventive security solutions given a set of preconditions and costs.
1.3.	Empirical
1.4.	Two expert panels and survey
2.1.	Pick-up and delivery van operations at a Belgian branch of a major express courier company.
2.2.	Unauthorized intrusion into pick-up and delivery vans. The threat is associated with theft and

	terrorism.
3.1.	A set of security solutions increasing protection of pick-up and delivery vans against unauthorized intrusion (Key card, audible alarm, silent alarm + GPS, notification on vehicles, awareness training, no company logos, formal instructions / compliance checks & sanctioning, double drivers, over security escorts.)
4.1.	N/A
4.2.	A set of preconditions influence outcomes of preventive security solutions: availability (legal, infrastructure), practicability (perceived), required knowledge, required expertise, user awareness, user belief, use commitment (anticipated), and co-operation.
5.1.	* Costs: Financial costs, ethical/social cost (labeling, distrust, civil liberties, inequalities), aesthetical cost * Reverse effects: Displacement (geographical, temporal, target, tactical, crime types), escalating effects, creative adaptation, and enticement effects

Hameri and Hintsa 2009

Assessing the Drivers of Change in Cross-border Supply Chains, International Journal of Physical Distribution and Logistics Management

Data field	
1.1.	International trade has been expanding rapidly over past decades and is still growing. For the sake of better governance and management, it is necessary to identify trends that shape the future international logistics management.
1.2.	To identify key drivers of change for cross-border trade and supply chains.
1.3.	Empirical
1.4.	Interviews (33) + Delphi panel (12)
2.1.	Global trade
2.2.	N/A
3.1.	N/A
4.1.	N/A
4.2.	N/A
5.1.	N/A

Joossens and Raw 2008

Progress in combating cigarette smuggling: controlling the supply chain, Tobacco control

Data field	
1.1.	Large scale organized tobacco smuggling causes significant revenue losses for governments and leads to increased tobacco consumption and associated health problems.
1.2.	To present how authorities in Italy, Spain, and the UK have managed to tackle large-scale illicit tobacco trade.
1.3.	Review

1.4.	Three country cases based on secondary data sources.
2.1.	European tobacco industry.
2.2.	Smuggling of untaxed cigarettes.
3.1.	A set of solutions including container screening, fiscal marks on cigarette packs, increased customs resources, and increased scrutiny of licit tobacco companies.
4.1.	* Tobacco companies changed their export practices under increased scrutiny of authorities. This disrupted the flow of cigarettes from licit manufacturers to illicit re-exporters. * Formal and legally binding agreements coupled with credible enforcement and threat of substantial sanctions.
4.2.	N/A
5.1.	Reduced smuggling.

Klima 2011

The Goods Transport Network's Vulnerability to Crime: Opportunities and Control Weaknesses, European Journal on Criminal Policy and Research

Data field	
1.1.	Cargo transport networks are clearly vulnerable for a variety of crime threats such as smuggling, cargo theft and terrorism. However, there have not been systematic studies that would have investigated what factors make the cargo transport networks vulnerable.
1.2.	To understand what makes cargo transport networks vulnerable to criminal activities.
1.3.	Empirical
1.4.	Structured interviews with 33 law enforcement agents and managers, four interviews with convicted criminals, 29 case fields form the Belgian Federal Police and customs services
2.1.	Focus on cross-border road transport from the Belgian perspective
2.2.	Smuggling of illegal goods (drugs, cigarettes, people), cargo theft and fraud against transport service providers (use of services without paying agreed compensation)
3.1.	A large variety of technologies, policies, regulations and procedures.
4.1.	N/A
4.2.	* "[Crime] opportunities for crime arise from weak sector conditions and weak regulations." * Weak sector conditions: self-employed drivers in financial distress are easier to solicit to smuggling jobs than established logistics enterprises with cash reserves, resources and skills to implement security solutions, monitoring systems and large customer base that enables them not accept dubious deals. * Regulatory weaknesses lead to lack of liability of logistics operators, inadequate law enforcement and absence of secure parking lots facilitate crime in the transport sector. * High security of large companies may displace cargo crime from protected targets to unprotected SME targets.
5.1.	N/A

Lee and Whang 2005

Higher supply chain security with lower cost: Lessons from total quality management, International Journal of Production Economics

Data field	
1.1.	SCS initiatives are generally seen as burden that drives costs and delays. It's necessary to search for solutions that assure high security of supply chains at low cost.
1.2.	To describe how the principles of total quality management can be used to design low cost high security supply chains.
1.3.	Analytical
1.4.	Queuing network modeling
2.1.	Focus on US-bound sea container traffic.
2.2.	Terrorist threat and world's logistics and transport systems.
3.1.	US SCS initiatives including C-TPAT, CSI and SST (Safe and Secure Tradeline). Specific security solutions include the advance manifest rule, RFID and container seals.
4.1.	N/A
4.2.	Security solutions that reduce length and variance of lead time.
5.1.	Reduction in pipeline inventories and safety stocks, decrease in inspection costs and pilferage, service level improvements through faster and more predictable lead times.

Lee et al. 2011

Supply chain efficiency and security: Coordination for collaborative investment in technology, European Journal of Operational Research

Data field	
1.1.	Information technologies may provide substantial benefits for companies in terms of better logistics efficiency and security. Despite of the fact, companies have not adopted such technologies as expected.
1.2.	To examine coordination problems and related incentive mechanisms between a manufacturer and a retailer when investing in technology that has potential to improve both logistics efficiency and security.
1.3.	Analytical
1.4.	Mathematical modeling with a two-echelon supply chain with a monopolistic retailer and on of its manufacturers
2.1.	N/A
2.2.	Product contamination
3.1.	Degree of investment in information technology (RFID in particular)
4.1.	
4.2.	* Relative strengths of efficiency and security concerns result in different coordination problems when implementing a technology. * Appropriate incentive mechanisms are contingent on the nature of coordination problems.

	* Imposing penalties on parties who is blamed for security breaches and tax incentives are ways to increase overcome coordination problems and reach optimal levels of investments.
5.1.	* Efficiency in terms of reduced replenishment lead time. * Security in terms of the time it takes to locate and eliminate the source of contamination.

Martens et al. 2011

Examining antecedents to supply chain security effectiveness: an exploratory study, Journal of business logistics

Data field	
1.1.	SCS research lacks quantitative empirical work. There is not, for example, little evidence about the association of management practices to SCS effectiveness.
1.2.	To explore the relationship between security management practices and the perceived effectiveness of SCS.
1.3.	Empirical
1.4.	Survey (69, 12%). Data analysis with principal component analysis and linear regression analysis.
2.1.	Resource-based view and supply chain integration
2.2.	US based firms (manufacturers, wholesalers/distributors and retailers)
3.1.	The authors operationalize SCS effectiveness as a function of effectiveness of a security program against cyber crime, terrorism, employee theft and theft by nonemployees (accidents and natural phenomena were dropped due to poor internal consistency).
4.1.	Security programs in general
4.2.	N/A
5.1.	* Hypothesized antecedents: Food company, proactive investment in SCS, resource constraints (lack of), management support (lack of), internal integration, external integration, perceived vulnerability of supply chain nodes, perceived vulnerability of supply chain links, employee training and the use of measurement / assessment * Significant antecedents in the light of empirical evidence (significant at .05 level): Food company and perceived vulnerability of node
1.1.	The authors assume implicitly that effective security programs result in protection against cyber crime, terrorism, employee theft and theft by non-employees

McClay and Dreiding 2012

Multilevel, threshold-based policies for cargo container security screening systems , European Journal of Operational Research

Data field	
1.1.	Terrorist may attack against the US through smuggling radioactive material into the country. Current inspection policies are suboptimal in terms of cost, delays and detection rate.

1.2.	To define optimal requirements for a primary screening alarm in multi-level container screening for radiological materials.
1.3.	Analytical
1.4.	Linear programming with knapsack problem models
2.1.	US bound traffic of containerized cargo
2.2.	Smuggling of radiological material into the US.
3.1.	Alarm thresholds for container inspection programs.
4.1.	N/A
4.2.	Circumstances under which primary screening alarms are triggered influence detection probability and inspection costs.
5.1.	Detection probability and screening budget.

Meixell and Norbis 2012

Integrating carrier selection with supplier selection decisions to improve supply chain security, International Transactions in Operational Research

Data field	
1.1.	Supply chain security is a major concern for logistics managers. However, current decision making models, that help managers to select suppliers and carriers, do not consider security as one of the decision criteria.
1.2.	To develop a methodology that incorporates security criterion into supplier and carrier selection process.
1.3.	Analytical
1.4.	Multi-criteria decision analysis
2.1.	N/A
2.2.	N/A
3.1.	Supplier's better security level.
4.1.	N/A
4.2.	N/A
5.1.	Trade-off between security, cost, quality and delivery reliability.

Merrick and McLay 2010

Is screening cargo containers for smuggled nuclear threats worthwhile? Decision analysis

Data field	
1.1.	Terrorist may exploit container traffic to smuggle nuclear and radiological material into the US. Deterrence effect of container screening seems to be little studied but important factor that affect the selection of container inspection policies.
1.2.	To examine additional screening objectives beyond cost and to investigate effect that screening has

	in discouraging terrorists.
1.3.	Analytical
1.4.	Multi-criteria decision analysis
2.1.	
2.2.	Terrorist smuggling nuclear devices and radiological material into the US.
3.1.	Radiation portal monitors designed to detect nuclear and radioactive material coupled with subsequent screening techniques such as X-ray and gamma imaging and physical inspections.
4.1.	Terrorist should be aware of screening policies.
4.2.	* Mounting a terrorist attack is expensive so increased screening and associated higher detection rate deters terrorist from exploiting container traffic (so called 'deterrence effect') * Multi-level screening process decreases the possibility of false alarm and resultant non-essential physical inspection.
5.1.	* Inspection related costs and delays. * Risk of smuggling in nuclear devices and radiological material

Murray-Tuite and Fei 2010

A methodology for assessing transportation network terrorism risk with attacker and defender interactions, Computer-aided civil and infrastructure engineering

Data field	
1.1.	
1.2.	To demonstrate a methodology for selecting and locating security solutions to protect transport systems from terrorism.
1.3.	Analytical
1.4.	Dynamic traffic assignment simulation with defender-attacker interaction. Demonstration with nominal data.
2.1.	
2.2.	Terrorist attacks against road transportation systems.
3.1.	Preventive and post-event security solutions. Intelligence on terrorist activities.
4.1.	N/A
4.2.	N/A
5.1.	* Both defenders' security solutions and terrorists' activities decrease capacity of a transport network and thus travel times. * Terrorist may substitute targets and attack methods in response to preventive security solutions.

Prokop 2012

Smart Containers and Public Goods Approach to Supply Chain Security, International Journal of Shipping and Transport Logistics

Data

field	
1.1.	Supply chain partners face different incentives to invest in security along supply chains. Private entities are inclined to under-invest in SCS from the society's perspective.
1.2.	To review current state of the smart container technology, assess its implications to SCS and use the economics of public goods to explain incentives for governments, shippers and carriers to engage in SCS.
1.3.	Analytical
1.4.	Economic analysis
2.1.	Economics of public goods
2.2.	US-bound sea container traffic
3.1.	Smuggling of weapons into the US
4.1.	Post 9/11 container security solutions, in particular smart container technologies, C-TPAT and CSI.
4.2.	N/A
5.1.	* Smart containers shipped from CSI-compliant ports by C-TPAT-certificated shippers and carriers are eligible for 'green line' treatment when they arrive at US ports. This reduces/eliminates due to customs formalities and may provide other benefits from the customs side (e.g. faster processing of duty drawbacks). * C-TPAT certificate could be seen as an insurance for companies that would allow them to be the first ones to resume shipping in the aftermaths of a major terrorist attacks. * Smart container technology has potential to mitigate the problem that some private companies may have an incentive to under-provide SCS.
1.1.	Trade off between efficiency and supply chain security.

Reilly et al. 2012

Game theory-based identification of facility use restrictions for the movement of hazardous materials under terrorist threat, Transportation Research Part E

Data field	
1.1.	Approximately 800.000 shipments of hazardous materials move in the US transport systems on a daily basis. Despite excellent safety records of hazmat carriage, there is always a risk that terrorists could exploit shipments of hazardous goods to mount an attack.
1.2.	To assist governments mitigate the risk of terrorism involved with the transport of hazardous goods.
1.3.	Analytical
1.4.	Game-theoretical analysis and demonstration with nominal data.
2.1.	US-transport networks with focus on rail infrastructure.
2.2.	Terrorists attacking shipments of hazardous materials
3.1.	Restrictions for the use of transport networks.
4.1.	Changes in regulatory environment of hazardous goods transport.
4.2.	Governments restrictions and prohibitions on transportation of hazardous goods influence behavior of terrorists (which links to use) and carriers of hazardous goods (which routings to use and how often).
5.1.	Carriers and terrorists change their behavior in response to government regulations.

Roach 2004

Initiatives to enhance maritime security at sea , Marine Policy

Data field	
1.1.	Maritime logistics is threatened by a myriad of security threats including hijacking, transport of dangerous weapons, migrant smuggling, and narcotics trafficking. International maritime law has certain weaknesses that prevent law enforcers to pursue illegal activities at seas.
1.2.	To propose amendments to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA).
1.3.	Review
1.4.	Legal analysis
2.1.	Shipping at international waters
2.2.	Hijacking, murder, narcotic trafficking, migrant smuggling, support for terrorist organizations, nebulous transactions involving dangerous weapons.
3.1.	Amendments to the SUA convention (Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation). The amendments focus on collaboration between coastal and flag states and legitimacy of ship boarding in case illicit activities are subjected to take place on board.
4.1.	Collaboration between flag and coastal countries enable prompt law enforcement intervention at seas in case illicit activities are suspected.
4.2.	N/A
5.1.	Increased capability to reduce crime and terrorism and associated violence at international waters.

Russel and Saldanha 2003

Five tenets of security-aware logistics and supply chain operation, Transportation Journal

Data field	
1.1.	The 9/11 terrorist attacks changed the way governments and companies think about supply chain risks. The heightened risk of transnational terrorism calls for new approaches for security-aware supply chain and logistics management.
1.2.	To develop principles for security-aware supply chain and logistics management under the heightened risk of terrorism.
1.3.	Review
1.4.	Literature review (N/A
2.1.	US based supply chains
2.2.	Terrorism
3.1.	Business-private partnerships, collaboration with trading partners, mode-shifting capability, communication channels for crisis management, and military concepts of agility, reservists and pre-positioning. SCS initiatives like CSI and C-TPAT
4.1.	N/A
4.2.	N/A

5.1.	More secure and resilient supply chains.

Sheu et al. 2006

A voluntary logistics security program and international supply chain partnership, Supply Chain Management: an International Journal

Data field	
1.1.	Thousands of US companies have joined the C-TPAT program since its implementation in April 2002. There is much talk but little evidence about effects of C-TPAT membership to business performance, logistics security, among other effects.
1.2.	To investigate influence of C-TPAT certification on business performance, logistics security, and international supply chain collaboration, and identify antecedents of successful C-TPAT implementation.
1.3.	Empirical
1.4.	Multiple cross-sectional case studies (5). Data analysis: within case, cross-case and expert analysis
2.1.	Five US-based companies (freight forwarder/broker; import service provider; importer/retailer; transportation/freight forwarding; importer)
2.2.	Terrorism
3.1.	C-TPAT
4.1.	Cross-functional teams, education and top management support were deemed indispensable in the implementation of C-TPAT.
4.2.	N/A
5.1.	* Four out of five case companies reported faster inspections at borders, reduced costs and increased customer satisfaction (the fifth company could not state any benefits due to very recent implementation of the program). * C-TPAT certification increases international collaboration with supply chain partners in terms of regular visits, communication, sharing of visions and education and training. Effects of the C-TPAT to logistics security were unclear.

Signoret 2009

On Cargo Security Solutions and Trade Costs, Global Economy Journal

Data field	
1.1.	Supply chain security initiatives have had tremendous impact on global trade and supply chains. However, there is little evidence about effects whether and to what extent SCS initiatives hinder international trade.
1.2.	To examine impact of CSI on import costs and cross-border trade.
1.3.	Empirical
1.4.	Longitudinal analysis of containerized imports into the US by port and country of origin from 1999 to 2006.
2.1.	US-bound containerized freight traffic

2.2.	Terrorists smuggling weapons into the US in containers
3.1.	CSI
4.1.	N/A
4.2.	N/A
5.1.	Data set does not provide significant evidence that CSI influences trade flows or incurs additional costs for US containerized maritime imports.

Speier et al. 2011

Global supply chain design considerations: Mitigating product safety and security risks, Journal of Operations Management

Data field	
1.1.	Supply chain disruptions are costly. There are little research that discusses what supply chain design strategies that would have potential to mitigate the risk of disruptions.
1.2.	To identify types of SCS strategies and examine how contextual factors influence their selection
1.3.	Empirical
1.4.	* 75 qualitative interviews with managers representing 25 companies in food, pharmaceutical and hazardous goods sectors, cross-sectional * Survey (n=199, usable response rate 14%), cross-sectional * Validating case study with the Dow Chemical company.
2.1.	Mainly food sector but also pharmaceutical and hazardous goods companies in the USA.
2.2.	Supply chain disruptions arising from intentional and unintentional risk sources.
3.1.	General solutions that improve product safety and security.
4.1.	N/A
4.2.	Depth and breadth of security initiatives depend on top management mindfulness, operational complexity, product risk and coupling.
5.1.	N/A

Staake et al. 2009

The Emergence of Counterfeit Trade: a Literature Review, European Journal of Marketing

Data field	
1.1.	Counterfeiting is a major problem at many industries. However, the nature and mechanisms underlying the trade in counterfeit products are largely unknown.
1.2.	To review literature on economics of counterfeit trade and underpinning supply chains.
1.3.	Review

1.4.	Literature review (> 45)
2.1.	Cross-industry
2.2.	Trafficking in counterfeits
3.1.	N/A
4.1.	N/A
4.2.	N/A
5.1.	N/A

Sternberg et al. 2012

Enhancing security through efficiency focus- Insights from a multiple stakeholder pilot implementation, Journal of business logistics

Data field	
1.1.	Efficiency and security are said to be opposing factors in logistics operations. Yet, it is claimed that information technologies could improve efficiency and security simultaneously
1.2.	To investigate whether and to what extent increased attention to efficiency results in improved security in carrier operations in a seaport context.
1.3.	Empirical
1.4.	Longitudinal case study with field pilot implementation
2.1.	Post-hoc linking to supply chain collaboration and information sharing literature
2.2.	Carrier operations in connection with port terminals carrying out RoRo operations on trailers at the port of Gothenburg.
3.1.	Mainly theft and smuggling.
4.1.	A set of solutions designed to improve efficiency. The main components are: * Information sharing through a common information area * Real-time geographical position of truck and trailer * Identification technology in truck, RFID tags on transport units and RFID readers mounted on terminals * Electronic manifest * E-Seal
4.2.	N/A
5.1.	* Increased efficiency in terms of reduced waiting times and increased ability to plan port operations (pre-arrival notification) and fast positioning of trailers in a port. * Increased security in terms of more secure document handling (decreases the risk that sensitive information falls into the hands of criminals), better anomaly detection (helps customs identify trailers that are most likely tampered in-transit) and increased visibility. * Both efficiency and security benefits actualize simultaneously.

Talas and Menachof 2009

The Efficient Cost between Security and Cost for Sea Ports: a Conceptual Model, International Journal of Risk Assessment and Management

Data field	
1.1.	Since the "9/11" terrorist attacks, operators of seaports and terminals are forced to increase their security levels. However, there is a lack of management tools that would assist managers in selection of cost-efficient SCS solutions.
1.2.	To develop a methodology that allows ports and port terminals to select a cost-efficient mix of SCS solutions.
1.3.	Analytical
1.4.	Markowitz theory on portfolio selection
2.1.	Seaports and terminals
2.2.	Crime in sea ports and port terminals, in particular terrorism
3.1.	A variety of security solutions that can be deployed in a port environment including perimeter fencing, security gates, CC-TV systems, security alarms, and X-ray scanners.
4.1.	N/A
4.2.	Security solutions incur costs.
5.1.	Costs and reduction in security risk levels.

Urciuoli 2011

Investing in Transport Security Solutions: Using the Quantitative Risk Assessment (QRA) Approach, International Journal of Risk Assessment and Management

Data field	
1.1.	Companies face increasing pressure to enhance security of their supply chains due to increasing cargo theft rates, risk of terrorism and mandatory security regulations. At the same time, managers are challenged to select cost-effective solutions among a broad set of security solutions.
1.2.	To demonstrate feasibility of a quantitative risk assessment methodology for selecting cost-effective security solutions against cargo theft
1.3.	Analytical
1.4.	Quantitative risk assessment approach where statistics and expert panels are used to determine parameter values of the decision model.
2.1.	Focus road transportation in Sweden.
2.2.	Cargo theft and its several modus operandi including burglary, robbery, hijacking and fraud.
3.1.	A variety of anti-theft solutions including mechanical locks, vehicle immobilizer, reinforced vehicle structured, and tracking solutions.
4.1.	N/A
4.2.	Security solutions drive cost and reduce risk of cargo theft.
5.1.	Trade-off between cargo theft risk level and monetary cost.

Van Weele and Ramirez-Marquez 2011

Optimization of Container Inspection Strategy via Genetic Algorithm, Annals of Operations Research

Data field	
1.1.	Given the huge number of containers arriving into the US ports, inspections of containerized cargo for explosives, drugs and other contraband is a daunting task. There is need to streamline and optimize current inspection strategies.
1.2.	To present an optimization technique for developing a container inspection strategy that provides specific detection rate at minimum cost.
1.3.	Analytical
1.4.	Decision analysis with a genetic algorithm
2.1.	Maritime logistics
2.2.	Contraband smuggling
3.1.	Variations of strategies for container inspection.
4.1.	N/A
4.2.	Sensor placement and sensor thresholds influence significantly detection rate and inspection costs.
5.1.	Detection rate and costs.

Voss et al. 2009b

The Role of Security in the Food Supplier Selection Decision, Journal of Business Logistics

Data field	
1.1.	The risk of supply chain disruptions has become more substantial in the post-9/11 environment with the heightened risk of terrorism. As disruptions are costly, companies might be willing to trade off price and other qualities for security when selecting suppliers.
1.2.	To investigate whether and under what conditions purchasing managers of US food companies are willing to trade off price and delivery reliability for security of suppliers' supply chains.
1.3.	Empirical
1.4.	* Over 20 qualitative interviews for exploration. * A conjoint analysis with product quality, product price, delivery reliability and supplier security competence as conjoint factors to reveal purchasing managers' preferences on suppliers' attributes. Respondent analyzed 15 conjoint scenarios.
2.1.	US food industry (manufacturers, distributors, retailers and logistics service providers)
2.2.	Threat of product contamination in food supply chains.
3.1.	Security of suppliers' supply chains
4.1.	N/A
4.2.	Security concerns and international sourcing increase willingness to trade off price for security domestically and price and delivery reliability for security internationally.
5.1.	Research is based on the premise that security solutions incur cost and increase prices for logistics services.

Voss et al. 2009a

The role of strategic security: internal and external security solutions with security performance implications, Transportation journal

Data field	
1.1.	Securing supply chains from disruptions arising from intentional or unintentional sources is important in the today's markets. There is not much information whether companies placing strategic priority on security perceive higher level SCS implementation and performance.
1.2.	To investigate whether high level of strategic priority on SCS is associated with high levels of SCS implementation and performance.
1.3.	Empirical
1.4.	* Interviews * Survey. Analysis with exploratory factor analysis and cluster analysis
2.1.	US food industry (manufacturers, distributors and retailers)
2.2.	Product contamination/security incident
3.1.	Information technologies such as RFID that enhance firms' capabilities to prevent, detect and respond to contamination and security incidents.
4.1.	N/A
4.2.	High level of strategic priority on security is associated with higher level of security implementation, external security collaboration and security performance.
5.1.	N/A

Wein et al. 2006

Preventing the Importation of Illicit Nuclear Materials in Shipping Containers, Risk Analysis

Data field	
1.1.	Terrorist may exploit shipping containers to smuggle nuclear weapon into the US. Current inspection policies seem to be suboptimal in terms of detection probability, port congestion and cost.
1.2.	To find optimal inspection strategy for detecting smuggling of nuclear material with a 11-layer security system.
1.3.	Analytical
1.4.	Queuing network and game-theoretical modeling
2.1.	US-bound container traffic
2.2.	Smuggling of nuclear material into the US in sea containers.
3.1.	"11-layer security system" comprising shipper certification, container seals, targeting software, passive (neutron and gamma), active (gamma and radiography) and manual testing in US and foreign ports.
4.1.	N/A
4.2.	* Inspections in oversea ports cost c.a. five times more than in US ports. * High-energy x-ray radiography and elongation passive neutron tests in oversea ports reduce costs significantly.

	* Key cost driver is the manual testing labor.
	* Terrorists' capability to shield nuclear weapons affects detection probability.
5.1.	Trade-off between port congestion, budget and detection rate of smuggling attempts.

Whipple et al. 2009

Supply chain security practices in the food industry: Do firms operating globally and domestically differ? International Journal of Physical Distribution and Logistics Management

Data field	
1.1.	Securing supply chains from disruptions arising from intentional or unintentional sources is important in the today's markets. There is not much information whether companies having international supply chains differ from companies having domestic supply chains in terms of managerial attention to SCS and engagement with supply chain partners in security related verification and information exchange.
1.2.	To explore association between SCS and firm performance in terms of security outcomes, product quality and customer service, and to compare whether firms having international supply chains place greater importance on security and are more likely to engage with their supply chain partners than firms with domestic supply chains.
1.3.	Empirical
1.4.	* Interviews (n=50), cross-sectional
	* Survey (n=199), cross-sectional
2.1.	US food sector (manufacturer, distributor or retailer)
2.2.	Product contamination/security incident
3.1.	N/A
4.1.	N/A
4.2.	Managers, who work for companies having international supply chains, perceive that their firms place higher importance on supply chain security and collaborate and monitor their supply chain partners more than managers who work for companies with domestic supply chains.
5.1.	Managers, who work for companies having international supply chains, perceive better security performance in terms of increased ability to detect and recover from SCS incidents than managers who work for companies with domestic supply chains.

Williams et al. 2008

Supply chain security: an overview and research agenda, International journal of logistics management

Data field	
1.1.	SCS has become a critical element in firms' overall supply chain risk management strategies. There

	is need for a comprehensive review on SCS studies in order to set agenda for future research.
1.2.	To give an overview on SCS research and set a research agenda.
1.3.	Review
1.4.	Literature review (32)
2.1.	N/A
2.2.	N/A
3.1.	N/A
4.1.	N/A
4.2.	N/A
5.1.	N/A

Williams et al. 2009b

Supply Chain Security Culture: Measure Development and Validation, the International Journal of Logistics Management

Data field	
1.1.	Companies are increasingly devoting attention to SCS. Previous research suggests that security-oriented culture is important for the firms to protect their supply chains. Yet, there are not reliable and valid scales that would measure the degree of supply chain security culture in an organization.
1.2.	To develop and validate a scale for measuring SCS culture.
1.3.	Empirical
1.4.	Scale development including surveys for pretesting (62, 29%) and scale validation (62, 3.5%)
2.1.	N/A
2.2.	N/A
3.1.	N/A
4.1.	N/A
4.2.	N/A
5.1.	N/A

Williams et al. 2009a

Why all the changes? An institutional theory approach to exploring the drivers of supply chain security (SCS), International Journal of Physical Distribution & Logistics Management

Data field	
1.1.	SCS has become a critical element in firms' overall supply chain risk management strategies. However, it is not clear what are the external sources of pressure that drive companies invest and

	engage in SCS.
1.2.	To identify external sources of pressure that drive firms to engage in SCS
1.3.	Empirical
1.4.	Interviews (17), cross-sectional
2.1.	US-based companies from multiple sectors
2.2.	N/A
3.1.	N/A
4.1.	N/A
4.2.	N/A
5.1.	* SCS efforts help improve relationships with governments, customers, and society. * By investing in SCS, a firm signals its intention to act as a good corporate citizen. * SCS investments, among other things, may bring more business opportunities, result in lower governmental scrutiny, and protect brand.

Yang and Wei 2013

The effect of supply chain security management on security performance in container shipping operations, Supply Chain Management: An International Journal

Data field	
1.1.	SCS management is key for competitiveness of container shipping operations. However, there is little evidence about effects of SCS management to security performance.
1.2.	To identify dimensions of security management in the Taiwanese container shipping sector and evaluate impact of each dimension to security performance.
1.3.	Empirical
1.4.	Survey (85, 48%), exploratory factor analysis and multiple regression analysis
2.1.	The Taiwanese shipping sector
2.2.	Maritime related crime.
3.1.	A variety of technologies and procedures that comprise SCS management system (e.g. CC-TV, anomaly reporting, business partner evaluation, background checks for employees)
4.1.	N/A
4.2.	* Partner relationship management has an impact on customs clearance performance. * Information management and partner relationships management has an impact on safety performance.
5.1.	Decrease in injuries, cargo loss and damage, equipment failure, frequency of accidents, waiting times at the borders, and number of customs inspections. Increase in cargo flow.

Yang et al. 2009

Use of Fuzzy Evidential Reasoning in Maritime Security Assessment, Risk Analysis

Data field	
1.1.	Most decision making tools lack capability to make use of diverse data and deal with high degree of uncertainty. Thus, there is need for a management framework that to make sense of subjective expert information in a systematic way.
1.2.	To develop tool, that can deal with subjective expert information and function under high degree of uncertainty, to facilitate the selection of security solutions.
1.3.	Analytical
1.4.	Multi-criteria decision analysis with fuzzy evidential reasoning
2.1.	Maritime logistics
2.2.	Terrorism
3.1.	N/A
4.1.	N/A
4.2.	Risk mitigation, technical requirements, implementation time and cost affect attractiveness of a given security measure in the applied fuzzy reasoning model.
5.1.	N/A

Annex C | Curriculum Vitae

Toni Männistö

Chair Management of Network Industries (MIR)
École Polytechnique Fédérale de Lausanne (EPFL)
Odyssea Building / Station 5 / 1015 Lausanne – Switzerland
+41 79 904 40 77/ toni.mannisto@epfl.ch

Academic education

09/2011 - to date	**PhD candidate at the Chair Management of Network Industries**
09/2007 - 09/2011	**MSc in Industrial Engineering and Management, Aalto University School of Science and Technology** Grade: 4,54 (5 = best, 0 = worst), graduation with distinction

Relevant Prior Work Experience

09/2009 – 12/2013	**Researcher, Cross-border Research Association**
11/2010 - 05/2011	**Business developer, Orion Pharma Oy**
05/2009 – 08/2009	**Research Assistant, Aalto University School of Science and Technology**

Peer-reviewed research articles

Männistö, T., Hintsa, J., Urciuoli, L. (2014). Supply Chain Crime – Taxonomy Development and Empirical Validation, *International Journal of Shipping and Transport Logistics, 6*(3), 238–256.

Urciuoli, L., Männistö, T., Khan, T., & Hintsa, J. (2013). Supply chain cyber security: Potential threats. *Information & Security: An International Journal*, *29*(1), 51-68.

Hintsa, J., Männistö, T., Urciuoli, L., & Granqvist, M. (2012). Future development of e-Customs: a survey study with Swiss companies. *International Journal of Electronic Government Research*, *8*(4), 1-13.

Selected reports and conference proceedings

Männistö, T. (2013). Rethinking the Postal and Courier Services as Critical Infrastructure. *Network Industry Quarterly*, *15*(4), 16-19.

Männistö, T. (2013). Restructuring Security and Customs Controls for a seamless Cross-border postal service. *Postal Industry Regulation*, *1*(2), 6-8.

Männistö, T. (2013). What Is the European Union Doing for Better Airmail Security? *Postal Industry Regulation*, *1*(1), 10-13.

Männistö, T., Finger, M. (2013, August). Assessing Stakeholders' Interests in Postal Security. *International Conference on Postal and Courier Services*, Venice, Italy.

Hintsa, J., Männistö, T., Urciuoli, L., Ahokas, J. (2012, May). Does better visibility help mitigate security risks in cross-border supply chains? - Case FP7-CASSANDRA. *e-Freight Conference 2012*, Delft, the Netherlands.

Hintsa, J., Männistö, T., Urciuoli, L., Ahokas J. (2011, December). Customs perspectives on detection of deliberate regulatory violations in global supply chains - the role of information and data in risk identification. *OSCE-UNECE Round Table/UNECE Inland Transport Security Forum*, Vienna, Austria.

Language skills

Finnish	Excellent
English	Excellent
French	Conversational
Swedish	Basics
German	Basics