Transport Reviews

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ttrv20

Innovation, transport security and supply chains: a review

Nicola De Liso & Luca Zamparini

To cite this article: Nicola De Liso & Luca Zamparini (2022) Innovation, transport security and supply chains: a review, Transport Reviews, 42:6, 725-738, DOI: 10.1080/01441647.2022.2105415

To link to this article: https://doi.org/10.1080/01441647.2022.2105415

Published online: 25 Jul 2022.

TRANSPORT REVIEWS
2022, VOL. 42, NO. 6, 725–738
https://doi.org/10.1080/01441647.2022.2105415

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

Innovation, transport security and supply chains: a review

Nicola De Liso and Luca Zamparini

Department of Law – Economics Division, University of Salento, Lecce, Italy

ABSTRACT

The recent decades have witnessed a progressive increase of global supply chains that have been related to most produced goods. Within this phenomenon, transport security has gained more and more importance, also because of the threats coming from organised crime and international terrorist groups. In this context, many stimuli have fostered investments on innovative technologies involving all transport modes. Some innovations are mode-specific while others are common to all of them, as in the case of cyber-security. On the basis of a thorough review of the literature, the main aim of the paper is to consider the impact of transport security innovations on supply chains, especially in terms of time and of economic costs. It emerges that momentous consequences can be generated by a security breach for all the firms and regions whose economic activities are reliant on the supply chain. The main implications of the analysis are that it is then necessary a coordination and collaboration among several private and public stakeholders, not only at the local and national level, but also at the supranational level. Moreover, the trade-off which may exist between the implementation of stricter security protocols and the impact on the speed and on the cost of supply chain activities must be taken into account.

ARTICLE HISTORY
Received 30 July 2020
Accepted 19 July 2022

KEYWORDS
Technology; innovation; transport security; transport modes; supply chains

1. Introduction

By looking at the evolution of aviation, maritime and land transport in the last decades, an extraordinarily rich landscape displays the accomplishments and potential of technology and innovation. Furthermore, the way in which technologies have been connected, particularly through ICTs, constitutes a further interesting branch of research. Traditionally, safety-related issues have been intrinsic to technological change. For instance, the very early marine steam-engines could actually be dangerous, and the technology was developed to make engines themselves safer, more reliable and fuel efficient. However, the international context, particularly after the September11th 2001 terrorist attack, has obliged firms and governments alike to consider with special emphasis the security dimension in general (CRISP, 2016) and of transport and supply chains specifically (PwC, 2011). The latter dimension has always characterised transport activities – the history of transport is also the history of piracy, of armed robbery and other transport-connected misdeeds – but since 2001 awareness has increased and much more attention has

CONTACT Nicola De Liso nicola.deliso@unisalento.it Department of Law – Economics Division, University of Salento, Via per Monteroni snc, Lecce 73100, Italy

been devoted to security. In this context, technology and innovation have gained and will continue to gain a very relevant role. While developing new technologies, agents must systematically consider the possibility of intentional actions aimed at disrupting the normal course of action. Security, though, does not only mean terrorism. In fact, it has many dimensions, which range from the above-mentioned piracy to human trafficking, from weapons and drugs smuggling to theft and pilferage, besides deliberate attacks to nations, governments, political and religious symbols, companies, and individuals. Moreover, technological innovations have to be carefully devised and handled given that they may minimise the exposure to (lack of) security-related acts but they may also determine a higher probability to incur in security breaches, as in the case of IT (Higgs, Pinsker, Smith, & Young, 2016).

When supply chains are taken into account, security innovations and their implementation must go beyond the consideration of single transport modes. A first methodological review, stating the new emphasis on security in supply chains, has been proposed by Gould, Macharis, and Haasis (2010). They stated that investing in security is important to improve response and resilience to accidents but also for the efficiency of business processes. At a more general level, specific attention has to be devoted to the nodes of transport networks, such as the intermodal terminals, given the difficulty to efficiently safeguard them and the momentous economic consequences that would originate in the short and in the medium term from successful attacks to these transport infrastructures (Zamparini, 2016). Secondly, the effective security of the supply chains requires the coordination and collaboration of several private and public stakeholders. In this context, it is important to focus on two main principles: openness and interdependence. With regard to the degree of openness, let us explain it by considering two examples which are at the two extremes of the range. Consider first *aviation*: given the nature of air travel – characterised by a relatively limited number of entry and exit points to the system –, this can be considered as a relatively closed system; on the opposite extreme, i.e. widely open, are networks such as rail and underground systems which are readily accessible to large numbers of people (UK-GsR, 2006). One expects that the more open a system is, the more is vulnerable to deliberate attacks.

Interdependence must be considered in at least two dimensions. The first one is related to the interdependence between the infrastructures and the components of the transport system – as an instance one can think of a freight train connected with a port to deliver steel products. The second dimension concerns the broad interdependencies which develop between the transport system and the economy and the regional economic systems, made up of communities, businesses and individuals.

A further aspect that must be considered concerns the different technologies which characterise each specific means of transport, because different technologies can constitute a preferred target in terms of the "easiness" with which that target can be hit, or because of the magnitude of the damage that terrorists expect to create. Three examples can clarify the previous statement. If the target is a running train, the effect of an attack will likely be much more devastating if the stricken train is a high-speed one – as opposed to a traditional train. If one wants to sabotage the engines of an aircraft, the degree of easiness may be different, and different skills required, according to whether that aircraft is a traditional piston-propeller, turboprop or turbojet one. The explosion inside a port of a vessel using liquefied natural gas as fuel may be much more devastating than a similar

event occurring on a vessel using marine diesel. Obviously pointing to each specific technology is only part of the problem, but this must be explicitly stressed.

The discussion mentioned above has highlighted the linkages between innovation and security in transport activities and in supply chains. Moreover, the need to consider their multifaceted relationships has emerged. To the best of the authors' knowledge, no previous work has attempted to review all these possible interconnections in a systematic way. The present paper is based on a structured literature review of the core topics which emerge from the title of the paper itself.

To avoid any misunderstanding, let us emphasise that what is referred to here is the specific interplay between innovation and transport and supply chains security, i.e. we do *not* provide a broad discussion of what innovation is.

This having been clarified, let us point out that, in order to carry out this review, at first a thorough search through keywords was executed in order to retrieve the works dealing with transport security and innovation. In a second stage, all papers that were deemed to focus too loosely to the themes of this article were discarded. Put another way, this literature review considers the impact of transport security innovations on supply chains, especially in terms of economic and time savings and costs.

The paper is organised as follows. Section 2 addresses the relationships which may exist between transport and security. Section 3 considers four fundamental premises related to innovation and transport security. Section 4 will analyse the technologies applied to transport security and their evolution in order to minimise breaches of security and the consequent socio-economic effects. Section 5 will highlight the influence of transport security on global supply chains. The final section will propose some concluding remarks and some suggested further directions of research.

2. Musings on the relationships between transport and security

A series of items to be considered when one wants to carry out a threat assessment is provided in this section. The list is not meant as a step-by-step series of aspects to be taken into account – that is, the items should be considered in parallel.

The first item is related to the *intrinsic vulnerability* (Mattsson & Jenelius, 2015) of each specific means of transport considered in itself, that is the individual aircraft, train, vessel, truck, etc. (Yap, van Oort, van Nes, & van Arem, 2018). For example, cabin pressurisation is fundamental for aircrafts, and any alteration of the pressure control system or a hole in the fuselage of the aircraft can be fatal to the crew – and the passengers, in case of a passenger airliner. Creating the conditions for the blowing out of a tyre of a truck carrying hazardous materials may be a low-tech, very effective – from the terrorists' point of view – means to achieve the end. An exercise in order to make a list of intrinsic vulnerabilities for each means of transport can easily be carried out.

The second item concerns the specific vulnerability of each main component due to systemic technological connections – shortly *systemic sector vulnerability* (Anbumozhi, Kimura, & Thangavelu, 2020; Berdica, 2002; Hellstrom, 2007). Consider rail systems: here we have a system which consists of the train, the railroad tracks, the catenary – which is a subsystem in itself –, the computerised control system which governs the train and connects the train itself with the overall railroad communication and signalling system, the stations and the train drivers (Besinovic, 2020; Gedik, Medal, Rainwater, Pohl, &

Mason, 2014). Human care and intervention is less and less important – just think of driverless trains and trucks or to automatic landing systems on jet airliners – but where it still exists, it must be taken into account: too often emphasis is on "things", forgetting the humans involved.

The third item consists in considering the interconnections between the various sectors, that is the *overall systemic vulnerability* (Banomyong, 2005; Wan, Yang, & Zhang, 2018; Wang, Su, & Chin, 2021). Again, an example can be useful: consider a freightliner (train) carrying containers which contain half-manufactured goods to be loaded into a cargo ship (Blumel, Boevé, Recagno, & Schilk, 2008). Here we have two transport sectors – rail and maritime – which come into contact: as a minimum there must be an entry point to the port for the train, there must exist an infrastructure with tracks leading somehow close the ship which will be loaded by means of gantry cranes. Each step, from the entry into the port, to getting close to the cranes, to matching the movement of the train with that of the cranes must be authorised and co-ordinated. Obviously not all the sectors are directly technologically interconnected: the aviation sector may well be basically disconnected from the marine sector. However, one can easily conceive an example in which a container is transported by a cargo aircraft, loaded by a truck which delivers it to a freight train which, in the end, delivers it to a ship. In this way, we have a connection between air, road, rail and maritime transport.

The fourth item which must be considered, and which cuts across all transport sectors – and the economy as a whole –, is that of ICTs (Kapalidis, 2020). Usually this is referred to as *cyber security*. ICTs are ubiquitous, and in a few years the Internet has experienced a double acceleration by becoming the "Internet of things" and, now, the "Internet of everything". Computerised networks are fundamental in governing the individual transport systems as well as the transport system as a whole. New ways of connecting the various systems continuously emerge, while new technologies are also being continuously developed and made easily accessible, an important one for transport and logistics being the "radio frequency identification device", or RFID, technology. As we shall see later, opportunities and threats come together.

The fifth item concerns *what* is transported. Many analyses are available in the literature (e.g. Burns, 2016), starting from those concerned with dangerous goods – or hazardous materials – as defined in the UN so-called ADR guidelines in which nine classes, from explosives to corrosive substances are listed. Dangerous goods are obviously not the only interesting categories: just think of how attractive transport of precious metals is, from gold to uranium, or of other raw materials, commodities and semi-finished products. Whatever good we have in mind, this same good will be transported through different means, each characterised by its weaknesses (Gkonis & Psaraftis, 2010). As an instance think of gold, from the Australian mine to the jeweller's shop in London: the transport, leading to different stages of manufacturing, will likely include trucks, trains, aircrafts and/or ships, and the final road transport.[1]

3. Innovation and transport security: four fundamental premises

Before explicitly dealing with the issue of innovation in transport security, four preliminary aspects must be underlined.

First of all, when we deal with the issue of improving security in transport – which is basically synonymous with some form of technological progress – an institutional perspective, encompassing private organisations, public agencies, and administrative authorities must be thoroughly considered (Venus Lun, Wong, Lai, & Cheng, 2008). In this context, the role of countries, through their Parliaments and Governments, is fundamental in at least three ways. To begin with, through Laws and Acts, countries set legally binding conditions which must be complied with in order to participate in the transport network. Secondly, they often participate, directly through their agencies or indirectly through funding, in the development of security-connected technologies – frequently benefiting from defence-related technologies. Third, besides setting mandatory levels of security, they also provide economic incentives through which those same levels can be met. Moreover, supranational institutions, organisations and bodies – from the International Civil Aviation Organization (ICAO) to the International Maritime Organization (IMO), to the Union Internationale des Chemins de fer (UIC) – are fundamental in diffusing, standardising and harmonising the procedures and knowledge concerning security and the levels of security required (Altemoller, 2011). Furthermore, it is also necessary to consider other national or supranational relevant players with which it is necessary to interact and co-ordinate: just think of the International Telecommunication Union (ITU).

The second aspect which must be preliminarily reminded concerns the overlapping which may exist between safety and security (Pizzi, 2020). For instance, improving safety features of marine engines may imply a positive externality also for security, by making it more difficult for would-be saboteurs to damage the engine itself. Thus, it is important to consider explicitly this relationship to avoid needless duplications of efforts. Furthermore, many of the security precautions typically used to deter criminals are also effective against terrorists (UK-NaCTSO, 2014).

The third aspect concerns the public-private partnership (Bakshi & Gans, 2010). In the case of security this is, out of necessity, a very close relationship. Government and the transport industry working in partnership is necessary to raise standards, as the former alone cannot provide the security regime that is needed (UK-GsR, 2006), and firms, through their explicit and tacit knowledge, can actually be helpful in pointing to weaknesses which would otherwise be missed. Furthermore, when we come to security issues, firms are expected to comply with the rules not so much because they would face sanctions if they did not, but because they perceive it as strategically important to adhere to those rules.

The fourth premise concerns the "meaning" of security. In fact, since the September 11th 2001 Twin Towers terrorist attack, there exists a systematic bias which leads to focus mainly on terrorism and air transport. As we already mentioned in the introductory section, it is important to have clear the whole range of security issues which must consider first of all the types of crimes to be contrasted, from drugs smuggling to human trafficking, from piracy to hijacking or kidnapping for ransom payment, to specific subcategories such as the so-called "petro-piracy", and so on. The second aspect concerns the types of criminality: the means and tools of organised transnational criminality are much more sophisticated than the ones available to a one-off gang of robbers. Thus, it is important to make extensive reasoning on which the targets could be, what the desired result of the criminal intent would be and through which means it could be achieved.

4. Technologies and innovation applied to transport security

Through technology we want to monitor as best as possible the transport system in which we have to consider the physical infrastructures, the mobile units (aircrafts, vessels, trains, trucks), the people, what is transported, and the ICTs infrastructure.

The technologies available are manifold and, in certain cases, they may be combined to get a higher level of security. One aspect though, must be stressed from the outset: when dealing with security, there seems to be a bias towards listing and taking into account mainly high-tech solutions – to which we will also refer hereafter. However, one should never forget that low- and traditional-tech solutions must not be ignored: physical fences, mechanical locks, guard dogs and sniffer dogs can still do a lot to prevent, stop and mitigate criminal actions.

The first kind of technology we refer to can be collectively addressed as "visual technology". In this category, all the apparatuses which generate some form of "vision", from individual webcams to closed-circuit television systems, can be subsumed. These apparatuses can be installed everywhere, from terminals (e.g. airport, seaport, train station) to logistic platforms, to inside and outside any mobile unit (aircraft, vessel, train, truck), to entrances of whatever structure, and so on. Drones have also been equipped with cameras, thus allowing fully mobile vision from above.

The evolution through time of the quality of the images obtained is spectacular, as is the possibility to process these images with automatic means to get as much information as possible. In a few decades we have had the transformation from black-and-white blurred images to high-definition colour images. Individual infrared cameras can be bought for as little as thirty dollars. In recent years the so-called "intelligent vision system" has been developed, and it can detect unusual behaviour or unauthorised access – that is, the system is active in alerting the human minder of the apparatus that something is going wrong. Furthermore, facial recognition has also become a reality, and is being constantly improved through artificial intelligence.

The second kind of technology we consider is that of security scanners (Leone & Liu, 2011; McLay & Dreiding, 2012). There exist different types of scanners – which can scan human bodies, luggage and other objects – based on different technologies and which can provide more or less detailed imaging. The most widely visible scanners are the "walk-through body scanners" which are substituting the old metal-detector-cum-personal-search by security staff in airports. Scanners making use of X-rays are very effective and different versions have been tested, some of which capable of showing also items hidden in human cavities. It thus does not come as a surprise that body scanners have raised concerns on passengers' health, and these concerns relate also to low-radiation X-rays apparatuses which could be dangerous for frequent flyers and airline crews (the problem would not be as important for applications such as in seaports where passengers and crews would not walk through these apparatuses as often). On the other hand, X-rays inspection systems, given their non-destructive nature, are being widely adopted for inspection of cargo containers.

The third category of technologies can be classified under the heading "detectors, sensors and transducers" (Janssens-Maenhout, De Roo, & Janssens, 2010; Rizzo, Barboni, Faggion, Azzalin, & Sironi, 2011). This category partly overlaps with the previous one, while some devices are jointly used with the apparatuses recalled above. The list of

devices and technologies behind them is too long to be fully reported, and we limit ourselves to a few examples. These devices can reveal the presence of certain substances, of objects, changes in magnitudes such as temperature, pressure and humidity, the presence of motion, whether the volume or the level of the contents of many types of container has changed or the configuration altered. The technologies range from electromagnetic induction of metal detectors to ultrasound transducers for monitoring shipping containers, to gamma-ray detectors to detect the presence of nuclear devices, to infrared-energy used for many non-contact sensors. In the case of "special" concerns, such as the search for explosives and hazardous substances, different technologies, more and more sophisticated and having completely different technological bases, have been sought and developed. In fact, for the case of explosives, the technologies available range from ion spectrometry[2] to chemiluminescence, from laser to X-rays.

The fourth type of technology that we consider is the one concerned with the identification of persons, be they white- or blue-collar workers working in the terminals or any other activity connected with the operation of the transport network, crew members or passengers. The technologies available include various types of badges, identity documents such as passports and – since a few years – biometrics. There usually exists a distinction between the identification of workers on the one hand, and passengers on the other. The former usually make use of a badge – the image we have in mind is that of credit-card-sized ones –, the latter of some identification document such as a passport. Both types of identification tools have experienced a process of digitisation, thus providing more and more information on the person carrying them. Even the passport, which at first sight has not much changed, now must contain a microchip in which the digital image of the face and of the fingerprints of the owner are stored. The latter comment leads automatically to the use of *biometrics* as a tool for identification. Biometrics applications can be distinguished into two main types, namely physiological and behavioural (ICAO, 2015); the former is – at the present stage of technology – more reliable than the latter, and it can give rise to four forms of recognition: fingerprint, facial, iris and retinal. Each form of recognition is being increasingly used though the former two are much more widespread. To have an idea of the way in which biometrics is gaining ground let us just remind that the Office of Biometric Identity Management which belongs to the US Department of Homeland Security "holds more than 260 million unique identities and processes more than 350,000 biometric transactions per day".

The fifth type of technology to be considered is the omnipresent digital technology which we subsume under the heading *information and communication technologies* – or ICTs – in the plural. These technologies cut across each economic sector and have become essential also for transport. There is no single item – from individual mobile units to the transport network as a whole – that does not depend, in one way or another, on them. Software has become the universal intermediary which, through appropriate data elaboration and algorithms, transforms signals received from hardware – cameras, contact and non-contact sensors, etc. – into a result, be it the "go-ahead" for the ship to dock or for the aircraft to land, the acknowledgement of the presence of a hazardous substance or the matching of a natural person with a picture through facial recognition.

Since a few years we are experiencing the transition from a condition in which humans were important in taking decisions to another in which humans are marginalised – that is

from "computer-assisted" to "computer-led" actions. With fully-fledged artificial intelligence in sight (Crawford, 2021; Polson & Scott, 2018), human-free computerised decision taking, and consequent action will become the rule. The latter statement explains the obsession with cyber-security of all Governments and supranational organisations: any bug in the digital world can be an advantage for the criminals.

The final comment concerning the ICTs must be devoted to cloud computing. In fact, the endless development and use of digital technologies in transport systems – as in any other economic activity – has made it necessary to have more and more data storage space, data sharing and data processing capability. The solution to this problem has been found through "cloud computing" which, given the way the technology has been developed, gives a handful of giant private companies – the first names which come to one's mind are Amazon and Google – a power unimaginable only fifteen years ago: the American Central Intelligence Agency (CIA) makes use of Amazon's cloud computing facilities, and this gives the idea that in the partnership between the state and the private company, the latter seems to be now in command.

To conclude this section, let us point out that technologies aimed at security in transport have partly been conceived ad hoc – e.g. certain types of sensors, detectors and transducers – and partly adapted from other fields – e.g. use of X-rays. Security concerns have also led to the development of many ICTs applications which would have never been created, had these needs not existed – e.g. credential authentication technology applied at first in Boston airport in early 2020 which enhances detection capabilities for identifying fraudulent documents, accelerates passengers' identification and provides information on passengers' flight status (US-DHS, 2010, 2015, 2018, 2020).

5. Impact of transport security innovations on global supply chains

An important aspect of transport security innovations is related to their impact on global supply chains, i.e. the combination of productive firms and service providers that control the raw material sourcing, the manufacturing activities, and the delivery of goods from the source of the commodities to the consumers (Closs & McGarrell, 2004). This is due to the fact that an attack on an important hub of a global supply chain – a port, an airport or a multimodal facility – does not only generate economic losses to the infrastructure itself, but it also determines momentous consequences for all the firms and regions whose economic activities are reliant on the flows of goods transiting in these important nodes (Prokop, 2012; Sheffi, 2001; Williams, Lueg Stephen, & LeMay, 2008). Among the arcs of the global supply chains, it is particularly important to control and enhance the security level of the main chokepoints in global shipping (i.e. the Straits of Hormuz and of Malacca, the Suez and Panama Canal).

The development of higher levels of security normally implies the coordination and collaboration among several private and public stakeholders, not only at the national and local but also at the international level (Cigolini, Pero, & Sianesi, 2016; Douglas Voss, Whipple, & Closs, 2009; Manuj & Mentzer, 2008). The main aim of this collaboration should be constituted by the heightening of the overall degree of resilience of the system, by minimising the likelihood of breaches to security and their related short term and long-term economic impacts. These are strongly conditioned not only by the ability of the

infrastructure/region to absorb the attack, but also by the level of support received during the recovery process from other nations and other transport actors.

In order to achieve the supply chain security goals, five interconnected dimensions must be jointly taken into consideration: ICTs security, process security, physical security, personnel security, and security partnership. Table 1 proposes a taxonomy of the main issues connected to these five dimensions.

It appears evident that an increased level of security depends, for three of these dimensions (ICTs security, process security and physical security), on the adoption of new technologies, strategies and activities. However, it must be taken into account that an important role is also deployed by the workforce that needs to be carefully chosen and constantly trained to the use of new technological devices (personnel security). Lastly, an important profile is represented by the security partnerships with suppliers and standard setters and authorities for the management of development and innovation of more efficient security standards. This is a particularly important issue. If the various transport firms that are involved in a supply chain consider their activities in isolation, the achievement of a satisfactory level of security will be much more difficult, especially in the intermodal hubs where the cooperation/collaboration of different stakeholders is more relevant.

A further important element to consider when shifting the attention to the global supply chains, is the trade-off which normally exists between the implementation of stricter security protocols on the one hand, and the (lower) speed and (higher) costs which emerge in the supply chain activities, on the other. Particular care must then characterise the choice and adoption of the most appropriate tools, devices and activities.

Table 2 proposes a categorisation of the innovations that have been described in Section 4 by partitioning them according to their impact on speed and on cost of supply chains. One dynamic aspect must be stressed from the outset: at first, security concerns prevail over cost and time considerations, that is in some cases the initial innovation successfully addresses the issue at stake – e.g. detecting explosives – but can be cumbersome and not as reliable, giving false positive results which, besides adding to the costs of inspection, slow down the handling process. Then, through R&D – which absorbs human and financial resources and takes time – faster, cheaper and better ways of addressing the

Table 1. Taxonomy of supply chain security profiles.

ICTs security	• Security enabling technologies • Vulnerability check • Accessibility
Process security	• Transport security • Handling security
Physical security	• Inventory security • Access control • Transport equipment
Personnel security	• Risk profile of job applicants and employees • Security training of employees • Security guidelines for employees
Security partnerships	• Partnerships with suppliers • Partnerships with standard setters and authorities • Supply chain management security standard development and innovation

Source: Authors' elaboration based on PWC (2011).

Table 2. Impact of innovation in transport security on supply chains' cost and time.

	Cost reduction	Cost increase
Time saving	• Object/container scanners • Detectors, sensors and transducers • Data elaboration and algorithms • Cloud computing • Advanced biometrics tools	• Individual webcams • Individual infrared cameras • Closed circuit television systems • Drones
Time consuming	• Full body scanners • Individual identification devices	• Early (cumbersome) biometrics tools • Early body scanners

Source: Authors' elaboration.

security issue are sought, thus shifting the classification of the innovation itself from "cost increasing *and* time consuming" to "cost reducing and time saving" – where this latter would be the standard idea of "innovation". Some security-induced innovations, though, may have immediately a positive effect in at least one of the two dimensions considered.

In some cases, the same technology (e.g. scanners) may have a positive effect in terms of time saving when it is related to objects or containers while it may imply more time-consuming activities if related to persons. Innovation of a specific technology (biometrics tools) has determined the passage from time consuming and cost increasing activities to relevant time and cost savings ones.

The most efficient innovations/technologies (implying both a reduction of costs and time saving) are the object/container scanners, the various detectors, sensors and transducers, the ICTs related applications (data elaboration and algorithm and cloud computing), and the advanced biometric tools. Other items, while time saving, may involve an increase in costs. They are the individual webcams and infrared cameras, closed circuit television systems and drones. However, it must be taken into account that an increase in the cost of security is normally counterbalanced by the reduction of risk that the security measure establishes by protecting or deterring a terrorist attack multiplied by the estimated overall cost of a successful security breach (Zamparini, 2018). This will determine a positive net benefit of the adopted technology/innovation. Lastly, body scanners, individual identification devices and early biometrics tools reduce supply chain costs but are more time consuming. In this case as well, the technology is normally implemented when its net benefit is pondered.

6. Conclusions

Transport security poses a series of questions, some of which find a solution in technologies already available in the system and which may be adapted to this specific use, while at other times these questions are specific to the transport system – the latter seen as a whole or as a set of components and links.

Starting from the broader perspective, one cannot avoid to refer to the complex relationships which exist between science, technology, society and the Governments. These latter play a broad and fundamental role, not least in trying to steer technology and its change (Lundvall, 1992; Mazzucato, 2015). Furthermore, it is important to point

out that technology creation and diffusion affects society, but many feedbacks exist from society to technology, so that we have an "intricate process by which technologies develop and become socially embedded, involving many actors across multiple settings and extended frameworks" (Williams, 2019, p. 140; see also Metcalfe & Ramlogan, 2005). Thus, besides the security aspects, Governments and regulators must reconcile different needs, which have to do with social acceptance of what is being implemented, issues of privacy, sometimes issues concerning health, while more and more attention is given in parallel to sustainability, that is energy efficiency and environmental impact.

While ideally Governments, security governmental agencies and regulators should stay ahead of threats, criminals have a clear advantage in that they do not have to worry about any of the issues just recalled. Furthermore, one must always remember that criminals have access to the same technologies as the legitimate agents, again with the advantage of not having to comply with any rule – whereas the latter have to.

When dealing with security, one fundamental aspect is threat assessment, which must consider at least four dimensions. The first consists in considering a detailed enumeration of possible criminal actions, from weapons and drugs smuggling to human trafficking, from theft to terrorist attack, etc. The second dimension consists in trying to evaluate which are the weak links of the security and supply chain, that is where the criminals will try to operate. The third dimension is that of trying to foresee which technological means the criminals might use. The fourth dimension concerns the possible answer(s) to the type of crime and technological means presumably used by the criminals.

Many technologies are available, and they can be combined to provide broader protection. Each technology is subject to improvement – *enhanced* detection capability, *higher* resolution imaging, and so on –, while new technologies have emerged, sometimes supplanting, sometimes complementing the existing ones. Innovation, though, often consists in using existing technologies and devices in different ways, an example being the use of ultrasound to detect whether a container door has been opened or if the level, configuration or volume of the goods has changed while in transit somewhere (Atlas, Cutter, & McVittie, 2008). And yet, it is of vital importance to be aware of the various types of vulnerability, which we addressed as intrinsic, sector and systemic.

Security emerges from a complex interaction of the security system – made up of the persons, agencies, rules, standards and technologies – with the broader socio-economic-legal system. Consistency of actions may be sometime difficult to be kept, as (too?) many aspects overlap. An example, inspired by UNCTAD (2020), may be useful to appreciate the latter comment. In fact, the whole spectrum of applicable maritime laws and regulations operates on the presumption of having a master and crew on board; however, these same laws and regulations are already partly obsolete, because they do not consider that already now remote-control crew working ashore is a reality. Furthermore, they run the risk to become quickly completely obsolete in the light of the development of artificial intelligence, likely leading to basically unmanned vessels. Future directions of research should address the innovation models and networks and the process of innovation deployment and diffusion. The issues emerging by adopting one possible typology and topology of innovation (e.g. centralised, decentralised, open or closed) should be considered carefully, possibly by adopting a multicriteria methodology. This analysis should include all possible objectives to be achieved in a seamless and efficient supply chain network. In particular, we need to strike a balance between highly prescriptive

total security and the need to ensure a free flow of trade (DNV, 2005). Talking specifically about those forms of terrorism which aim to bring our economies to a standstill, "if we put an anti-terrorist mindset on and make the protocol extremely cumbersome to avoid the terrorist event, we risk achieving the same outcome the terrorists desire" (Closs & McGarrell, 2004).

Notes

1. In the case of passenger transport, a sixth item would have to be explicitly considered, i.e. *who* is transported. In this context, terrorist attacks aimed at politicians or civilian passengers travelling by air, train or ship, and the actions aimed at creating difficulties to specific individuals (from CEOs to highly visible VIPs) should be taken into account. The possible aims of these acts would be attracting attention, simply creating disruption, kidnapping, and so on.
2. Worthy of a comment is the fact that ion spectrometry has been developed in different ways; for a review see Mäkinen, Nousiainen, & Sillanpää (2011).

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Altemoller, F. (2011). Towards an international regime of supply chain security: An international relations perspective. *World Customs Journal*, *5*(2), 21–34.

Anbumozhi, V., Kimura, F., & Thangavelu, S. M. (2020). Global supply chain resilience: Vulnerability and shifting risk management strategies. In V. Anbumozhi, F. Kimura, & S. Thangavelu (Eds.), *Supply chain resilience* (pp. 3–14). Singapore: Springer.

Atlas, L., Cutter, J., & McVittie, P. (2008). *Use of ultrasound for monitoring security of shipping containers*, Patent Application Publication No. US 2008/0047350 A1.

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

Banomyong, R. (2005). The impact of port and trade security initiatives on maritime supply-chain management. *Maritime Policy and Management*, *32*(1), 3–13.

Berdica, K. (2002). An introduction to road vulnerability: What has been done, is done and should be done. *Transport Policy*, *9*, 117–127.

Besinovic, N. (2020). Resilience in railway transport systems: A literature review and research agenda. *Transport Reviews*, *40*(4), 457–478.

Blumel, E., Boevé, W., Recagno, V., & Schilk, G. (2008). Ship, port and supply chain security concepts interlinking maritime with hinterland transport chains. *WMU Journal of Maritime Affairs*, *7*(1), 205–225.

Burns, M. G. (2016). *Logistics and transportation security. A strategic, tactical, and operational guide to resilience*. London: CRC Press.

Cigolini, R., Pero, M., & Sianesi, A. (2016). Reinforcing supply chain security through organizational and cultural tools within the intermodal rail and road industry. *The International Journal of Logistics Management*, *27*(3), 816–836.

Closs, D. J., & McGarrell, E. F. (2004). *Enhancing security throughout the supply chain*. Washington: IBM Center for the Business of Government Special Report Series.

Crawford, K. (2021). *Atlas of AI. Power, politics and the planetary costs of artificial intelligence*. New Haven: Yale University Press.

CRISP. (2016). *Taxonomy of security products, systems and services*. Final report of the EU project "Evaluation and certification schemes for security products", Seventh Framework Programme for Security (Grant number: 607941).
DNV. (2005). *Study on the impacts of possible European legislation to improve transport security*. A report for the European Commission DG TREN by Det Norske Veritas NV.
Douglas Voss, M., Whipple, J. M., & Closs, D. J. (2009). The role of strategic security: Internal and external security measures with security performance implications. *Transportation Journal*, *48*(2), 5–23.
Gedik, R., Medal, H., Rainwater, C., Pohl, E. A., & Mason, S. J. (2014). Vulnerability assessment and rerouting of freight trains under disruptions: A coal supply chain network application. *Transportation Research E: Logistics and Transportation Review*, *71*, 45–57.
Gkonis, K. G., & Psaraftis, H. N. (2010). Container transportation as an interdependent security problem. *Journal of Transportation Security*, *3*, 197–211.
Gould, J. E., Macharis, C., & Haasis, H.-D. (2010). Emergence of security in supply chain management literature. *Journal of Transportation Security*, *3*, 287–302.
Hellstrom, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science*, *45*(3), 415–430.
Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems*, *30*(3), 79–98.
ICAO. (2015). *Machine readable travel documents*. Montréal: International Civil Aviation Organization.
Janssens-Maenhout, G., De Roo, F., & Janssens, W. (2010). Contributing to shipping container security: Can passive sensors bring a solution? *Journal of Environmental Radioactivity*, *101*, 95–105.
Kapalidis, P. (2020). Cybersecurity at sea. In L. Otto (Ed.), *Global challenges in maritime security. Advanced sciences and technologies for security applications* (pp. 127–143). Cham: Springer.
Leone, K., & Liu, R. (2011). Improving airport security screening checkpoint operations in the US via paced system design. *Journal of Air Transport Management*, *17*, 62–67.
Lundvall, B.-A. (Ed.). (1992). *National systems of innovation*. London: Pinter.
Mäkinen, M., Nousiainen, M., & Sillanpää, M. (2011). Ion spectrometric detection technologies for ultra-traces of explosives: A review. *Mass Spectrometry Review*, *30*(5), 940–973.
Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192–223.
Mattsson, L.-G., & Jenelius, E. (2015). Vulnerabikity and resilience of transport systems. A discussion of recent research. *Transportation Research Part A: Policy and Practice*, *81*, 16–34.
Mazzucato, M. (2015). *The entrepreneurial state: Debunking public vs. private sector myths*. London: Anthem Press.
McLay, L. A., & Dreiding, R. (2012). Multilevel threshold-based policies for cargo container security screening systems. *European Journal of Operational Research*, *220*, 522–529.
Metcalfe, J. S., & Ramlogan, R. (2005). Limits to the economy of knowledge and knowledge of the economy. *Futures*, *37*(7), 655–674.
Pizzi, G. (2020). Cybersecurity and its integration with safety for transport systems: Not a formal fulfillment but ana actual commitment. *Transportation Research Procedia*, *45*, 250–257.
Polson, N., & Scott, J. (2018). *AIQ. How artificial intelligence works and how we can harness its power for a better world*. London: Bantam Press.
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.
PWC. (2011). *Transportation and logistics 2030. Volume 4: Securing the supply chain*. London: PWC. Retrieved 14 July 2020. https://www.pwc.com/gx/en/industries/transportation-logistics/publications/tl2030.html
Rizzo, F., Barboni, M., Faggion, L., Azzalin, G., & Sironi, M. (2011). Improved security for commercial container transports using an innovative RFID system. *Journal of Network and Computer Applications*, *34*, 846–852.
Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management*, *12*(2), 1–11.

UK-GsR. (2006). *The government's response to the house of commons transport committee's preliminary report*. London: The Stationary Office.
UK-NaCTSO. (2014). *Counter terrorism protective security advice for general aviation*. London: National Counter Terrorism Security Office.
UNCTAD. (2020). *Review of maritime transport 2019*. Geneva: United Nations.
US-DHS. (2010). *Transportation systems sector-specific plan. An annex to the national infrastructure protection plan*. Washington: US Department of Homeland Security – Department of Transportation.
US-DHS. (2015). *Transportation systems sector-specific plan*. Washington: US Department of Homeland Security – Department of Transportation.
US-DHS. (2018). *Advanced integrated passenger and baggage screening technologies. Fiscal year 2017 report to congress*. Washington: US Department of Homeland Security – Transportation Security Administration.
US-DHS. (2020). TSA at Boston Logan international airport gets new credential authentication technology to improve checkpoint screening capabilities. Internet document. https://www.tsa.gov/news/press/releases/2020/02/26/tsa-boston-logan-international-airport-gets-new-credential, US Department of Homeland Security – Transportation Security Administration
Venus Lun, Y. H., Wong, C. W. Y., Lai, K.-H., & Cheng, T. C. E. (2008). Institutional perspective on the adoption of technology for the security enhancement of container transport. *Transport Reviews*, *28*(1), 21–33.
Wan, C., Yang, Z., & Zhang, D. (2018). Resilience in transportation systems: A systematic review and future directions. *Transport Reviews*, *38*(4), 479–498.
Wang, B., Su, Q., & Chin, K. S. (2021). Vulnerability assessment of China-Europe railway express multimodal transport network under cascading failures. *Physica A: Statistical Mechanics and Its Applications*, *584*, 126359.
Williams, R. (2019). The social shaping of technology. In T. L. Pittinsky (Ed.), *Science, technology, and society* (pp. 138–162). Cambridge: Cambridge University Press.
Williams, Z., Lueg Stephen, J. E., & LeMay, A. (2008). Supply chain security: An overview and research agenda. *The International Journal of Logistics Management*, *19*(2), 254–281.
Yap, M. D., van Oort, N., van Nes, R., & van Arem, B. (2018). Identification and quantification of link vulnerability in multi-level public transport networks: A passenger perspective. *Transportation*, *45*, 1161–1180.
Zamparini, L. (2016). Economic issues in multimodal freight transport security. In J. Szyliowicz, L. Zamparini, G. Reniers, & D. Rhoades (Eds.), *Multimodal transport security: Frameworks and policy applications in freight and passenger transport*. Cheltenham: Elgar (pp. 35–47).
Zamparini, L. (2018). Economic issues in air transport security. In J. Szyliowicz, & L. Zamparini (Eds.), *Air transport security: Issues, challenges and national policies*. Cheltenham: Elgar (pp. 32–42).