The future security of travel of public transport: a review of evidence

Author: Dr Mark Beecroft, Centre for Transport Research, School of Geosciences, University of Aberdeen

Keywords: transport, security, future mobility, technology, crime

Abstract

This evidence review considers future security of travel by public transport and addresses three questions: (1) What are the current security challenges for public transport networks? (2) What are the emerging future security challenges? (3) What technologies will have the biggest impact on security of public transport in the future? The review identified current personal and operational security challenges associated with: convenience and privacy; interoperability and communication; risks and benefits of increasing connectivity; and skills requirements for the public transport sector.

Important emerging security challenges relate to: user and service provider security in a future of data-driven mobility; design and evaluation of security measures for all modes; knowledge-exchange and coordination in research and action to enhance security; and the need to better understand passenger behaviour, needs and attitudes in relation to travel, technology and security. The biggest impact technologies were identified as Vehicle (Unmanned Aerial Vehicles; Connected and Autonomous Vehicles and Electric Vehicles) and ICT (Internet of Things; social media; mobile platforms; Open Data, and Big Data). In relation to ICTs, impacts relate to connectivity and data sharing which represent both vulnerabilities and strengths. For vehicle technologies, automation and connectivity were the factors most influencing impact for good or ill.

Introduction

Security is important for public transport because it has the potential to influence travel behaviour at every stage of a journey from pre-trip planning, through undertaking the journey, to post-trip evaluation. In the UK context, it has been estimated that reducing fear of crime could increase public transport patronage by 3% at peak and 10% at off peak times (Newton 2004). There are a significant challenges in measuring crime and disorder on public transport, that make it difficult to determine whether a gap exists between the ‘perceived’ and ‘actual’ levels of crime (Newton 2004). This is a consequence of limitations of data collected on actual levels of crime on public transport. The degree to which under-reporting of public transport crime is an important factor is also unclear. It has been suggested that, reported crime is 25 to 30 times below the actual level of public transport crime (Levine and Wachs 1986 cited in Newton 2004). Alongside these concerns over data reliability and availability there is considerable volatility in public transport crime statistics, which relates to wider social trends. For example, the British Transport Police in 2018 reported significant rises in crimes committed on the railways compared to the previous year in relation to all crime (17%), violence against the person (26%), sexual offences (16%) and criminal damage (21%) (British Transport Police 2018).

Transport security is a multi-faceted concept, which can be subject to a range of interpretations. For the purpose of this review, the domain of transport security will be defined and this will form part of the determination of the scope of the review alongside the research questions. Security is defined in the Oxford English Dictionary as ‘freedom from danger or threat; the state or condition of being protected from or not exposed to danger; safety.” (OED Online 2017). The reference to safety is significant. Safety and security have traditionally been bundled together in the transport sector. There are undoubtedly strong synergies between transport security and safety. Beecroft and Pangbourne provide a conceptual framework for the definition of personal security which identifies confidence, safety and security as the three key aspects which overlap and intertwine in defining personal security: *"By combining these perspectives that participants implicitly or explicitly attached to personal security in relation to travel, we reach our definition, that personal security is an objective freedom from security and safety risks combined with a subjective freedom from fear and uncertainty."* (Beecroft and Pangbourne 2015a). Equally, the increasing focus on resilience as a conceptual approach has led to the common consideration of security and safety concerns when assessing vulnerabilities to external threats of transport systems, services and infrastructures (Reggiani 2013; EC 2017).

Accepting these synergies, it is necessary to establish some distinctions between security and safety for the review to be appropriately focused. Security issues can be separated from safety on the basis of intent (criminal or anti-social) and that they are exclusively man-made (Holtrop and Kretz 2008 cited in Reniers and Amyotte 2012).

This review recognises that security is an issue that operates at a range of spatial scales from the global to the household and individual level and every point in between. Indeed different spatial scales can be engaged in the course of a single door-to-door journey. It incorporates everything from personal security from crime and anti-social behaviour to national security in relation to terrorism (conventional warfare/military operations are considered out of scope of this review). The challenges faced at the range of scales covered by public transport security are extensive and their nature varies significantly at different scales. There may be solutions to security challenges at one scale that generate new challenges or exacerbate existing security challenges at other scales i.e. the priorities of national security and individual personal security may be quite different.

When considering the notion of public transport security it is important to appreciate what we are trying to keep secure. This can range from the individual and their property to public transport systems, services and infrastructures. When determining property we must consider both physical and virtual/digital property in the context of a world where there is ever-increasing convergence between the digital and physical experience and our digital and physical identities (TSC 2016). A final point of definition required is the distinction between current and emerging security challenges which pertains to research questions 1 and 2. In this review, current challenges are identified by research evidence that has been and is currently being undertaken. Emerging challenges are determined by evidence which identifies future issues for research and associated trends.

Methodology

This evidence review was completed in 2018 and was undertaken using systematic evidence review principles. The review combines the interrogation of academic and policy literature (both official and "grey" materials). The success of this review was partly dependent on the ability of the Investigator to identify key words and their variants which would lead to an efficient and effective search of material in relation to the three research questions.

In order to assess security challenges for public transport networks it is necessary to construct/adopt a typology for analysis. This review adopts the typology provided by the European Commission in its Research Theme Analysis Report on Transport Security (EC 2017). This typology is appropriate given that it has been applied to review the transport security research landscape in the most relevant, systematic and comprehensive manner currently available. This report reviewed European Union supported transport security related research, research financed nationally in the European Research Area Network and selected Global research programmes. It reviewed completed and ongoing projects since 2001. The typology is expressed in the form of a set of six transport security themes as follows:

1. Threat detection and prevention
2. Crisis management

3. Cyber security, privacy and ICT
4. Staff security training
5. Cargo security
6. Passenger security

The fifth theme, Cargo security was not adopted for the review given its exclusive focus on public (passenger) transport. The adoption of this typology does not imply an endorsement of the overarching strategy towards transport security, as Hoijtink (2015) states:

> *"European security research as a whole is performed in such a way that it becomes difficult to contest. In particular, the Seventh Framework Programme's twin rationale – enhancing the security of Europe's citizens, while enlarging the European market for civil security – is so dominant that it renders questions about its use, desirability and effectiveness obsolete. What kind of security are we investing in and against which costs? And, most importantly, what kind of security do we want, and for whom? These questions are not raised, but they have become ever more relevant now that the EU has intensified its investment in security research with the launch of the Horizon2020 project."*

Discussion under these themes includes coverage of security issues across modes including transition points (such as interchanges) for passenger transport. Whilst findings from EC research are the starting point for evidence review in each theme, this evidence base is extended to provide a broader geographical coverage (particularly through research evidence from North America and Australasia).

Findings (1): What are the current security challenges for public transport networks?

Threat detection and prevention

The EC reviewed 78 research projects on this theme. In terms of scope, it is notable that projects in the field of risk assessment and management have benefitted from fairly continuous research over the years as it requires constant revision/review in the light of changing vulnerabilities and threats. The introduction of ‘Efficiency’ as a research theme from 2009 and its continued emphasis is a recognition of a significant current challenge: to make threat detection and prevention more efficient and less disturbing to traffic flow, particularly in relation to passengers (EC 2017). Further research by Carter et al (2016) found that airport style screening was the least acceptable of a set of 10 proposed public transport security measures. It is particularly notable that research funding in the transport security field has typically been reactive rather than proactive. Research (and associated funding) has tended to respond to threats/events rather than seeking to anticipate them (EC 2017). This is a clear weakness and is unlikely to be confined to the European context.

The EC review of projects reveals that research in this field has tended to be focussed on aviation, but it is increasingly focussing on other modes (See also Cavallini et al 2014 for a discussion of the comparative lack of detailed security legislation in land-based transport when compared with aviation). Research has long focussed on monitoring and surveillance systems for aircraft, airports, passengers and luggage. An important identified challenge is how and when to transfer innovations in monitoring and surveillance from the air transport sector to other transport sectors, particularly as they are likely to impact significantly upon efficiency (EC 2017, see also Patil et al 2014).

Research in the road transport sector has largely focussed upon systems for unattended surveillance of public transport and on technologies and methods to better design stations and terminals to reduce the impact of security incidents. It is notable that in most recent years the protection of ‘Critical Infrastructure’ has been identified as a key challenge, reflecting “the need for a holistic approach, integrating functionalities at all critical infrastructure levels (i.e. individual, across interdependent critical infrastructure and across borders).” (EC 2017, see also Zamparini and Shiftan 2013; Reggiani 2013 and Cavallini et al 2014). This challenge has also been recognised in the United States by Szyliowicz (2013) who stated that the lack of an updated national policy to resolve the serious weaknesses of critical transportation infrastructure negatively impacts security.

Crisis management

The EC reviewed 31 projects on this theme. Research has tended to focus more upon organisation of crisis and emergency management (including recovery and resilience planning) rather than technological considerations. The key challenge in this regard is the intelligent linking of information sources and stakeholders and related issues of interoperability of procedures and technologies. This points to the need for cooperative working practices across borders (modal/spatial/governmental) to ensure effective collaboration and minimise the consequences of security-based emergencies. It also points to an identified future challenge in terms of the technologies needed to intelligently and securely link information (EC 2017). Beecroft and Pangbourne (2015a) noted that both resilience planning and crisis management were important current challenges and effective solutions were dependent on improvements in collaborative working and information sharing across the transport sector.

Cyber security, privacy and information and communications technology (ICT)

The EC reviewed 28 projects on this theme. Half of these projects have commenced in the last five years, reflecting the growing recognition of the fundamental and ever-increasing role that ICT plays in our transport systems, services and infrastructures (EC 2017, see also Cavallini et al 2014). Research in this theme was intitially predominatly in the aviation sector , but is increasingly spread to the road and rail sectors. Key focus areas include secure vehicle-to-everything (V2X) communication and associated privacy and security concerns (EC 2017, see also Azees et al 2016). When considered as a multi-modal issue within the context of smart cities, securing V2X communication is a significant challenge and cryptographic solutions are a focus for current research (Javed et al 2016).

Securing transport networks and infrastructures from cyber-threats is an increasing issue of research focus. Infrastructure and network control equipment is typically old legacy software and hardware whilst securing our critical infrastructure increasingly relies upon the newest interconnected ICT technologies and this raises significant integration challenges. (EC 2017). Personal identity protection and broader data protection are key issues for transport security. The Norwegian Data Protection and Privacy Implication in Road Safety project revealed survey respondents concerns about being exposed to misuse of personal data were greater than for terror attacks (EC 2017).

The UK Transport Systems Catapult (TSC 2016) undertook an evidence review combined with interviews and workshops with over seventy experts on cyber security and intelligent mobility (IM)[1] The review encompassed current practice and future priorities. In relation to current practice it found:

“All sectors of mobility realise that cyber security is a significant issue affecting operations and services. But this understanding is still not equivalent to the scale of the issue at hand. New cyber security strategies will be accelerated regardless of the conditions of the intelligent mobility market. But their impacts will be greatest where effective strategy to accelerate these technologies into intelligent mobility exist, and where industry culture enables it to do so.” (TSC 2016)

IM and its key domains of automation, new mobility models (particularly Mobility as a Service or MaaS) and smart ecosystems are particulalrly dependent upon complex and

[1] A concept which sees emerging technologies enabling smarter, greener and more efficient movement of people and goods (TSC 2016).

interconnected data networks that work across sectors and services making cyber security a key consideration (TSC 2016). The key current challenges identified by the TSC are: the establishment of principles for securing IM; development of technology and research roadmaps for securing IM; and upskilling the mobility sector workforce in cyber security (TSC 2016). In relation to automation, Petit and Shladover (2015) have explored potential cyber-attacks in relation to connected and autonomous vehicles.They identified GNSS spoofing and injection of fake messages as the most dangerous attacks in terms of both likelihood and severity.

Staff security training

The EC reviewed 28 projects on this theme. Significant challenges identified in this area include inconsistencies in skills education and training at varying scales: across countries and even between companies in the same regions. There are many examples of good practice in training, but transferability is inconsistent. At its worst, deficiencies in training have led to significant skills gaps and these can be exacerbated by increasing dependence on technologies to deliver staff training and to assist staff in customer service and problem resolution. Provision of training to handle complex situations can be difficult and an increasing need to understand and predict social behaviour under stressful emergencies has been identified as an important need in across transport modes. Again, aviation tends to lead the way and there is a need to address transferability challenges in incorporating best practice from that sector to other modes (EC 2017).

Passenger security

The EC reviewed 23 projects on this theme. Policy and research requirements have usually been developed in response to specific incidents rather than in a proactive manner and this is identified as a weakness (EC 2017). The predominant focus of research in land-based modes has been upon mass public transport, especially in urban areas (EC 2017). Demographic trends towards urbanisation combined with the increasing frequency and severity of terrorist incidents in these environments suggest this focus will need to intensify (Holgersson and Bjornstig 2014). Here, a major issue is the difficulty of implementing security measures whilst maintaining passenger flows through the network, particularly at large interchanges. This relates both to issues of threat detection (monitoring and surveillance), but also to responding to crises and providing effective information and support. Learning from aviation is again important here and also in relation to developing blast resistant materials for use in trains and metro carriages. The two main security challenges identified for land transport are "avoiding interruptions to transport networks as a result of terrorist attacks and ensuring that transport does not become a means for an attack." (EC 2017).

Findings (2): What are the emerging security challenges, looking out to 2040?

Threat detection and prevention

The EC identified that the public transport sector has previously paid limited attention to the detection and prevention of threats and associated system vulnerabilities compared to other modes (specifically aviation and maritime). This needs to change in the light of the growing scale of the threat (EC 2017). Learning from aviation in this regard represents both an opportunity and a challenge for reasons already outlined. However, Cole and Kuhlmann (2011) have argued that even in aviation a proactive approach (based on anticipatory scenario planning) is needed to identify future threats and their coverage by airport security processes and technologies.

Developing a more universal and collaborative approach to threat detection and prevention is a critical issue going forward in the context of increasing connected transport networks, services and infrastructures (EC 2017). Cross-border co-operation will be integral in this area and the uncertainty of arrangements post-Brexit clearly represents a significant challenge in the short to medium term in the European context.

Crisis management

An important emerging challenge in this theme identified by the EC was to maximise the exploitation of big-data applications to support crisis management in terms of gathering intelligence on emerging situations and then distributing that information effectively to stakeholders. Cross-sector research was also called for in relation to cascade effects to minimise risks to crisis management i.e. social media constitutes a core means of communication, but mobile networks can be subject to overload and even to potential misuse both deliberate and unintentional (EC 2017).

Steenbruggen et al (2013) investigated the use of data obtained from cellular-phone networks in supporting incident management, with particular attention to transport safety and security. They found that the use of telecom data has great potential to provide new types of information services. This could help to create an accurate understandable picture of reality to improve situational awareness. However, issues of timeliness, trust and provenance were significant emerging challenges.

Cyber security, privacy and information and communications technology (ICT)

The EC has identified intensive collaboration between different stakeholders in cyber security, privacy and ICT as the fundamental emerging challenge in this theme. More specifically the following emerging challenges have been identified:

> *"the phenomena of the Internet of Things and cloud computing represents potential sources of near-future threats, as huge financial investments and human resources are now being committed. Their impacts on data mining, the reliability of information, the ability to deliver in-time discovery and response capabilities, and*

> *privacy protection should be priorities for future European research and development activities."* (EC 2017).

The TSC (2016) has identified that the rapidly changing security and mobility landscape will mean significant growth in the number, frequency and severity of cyber-attacks in the transport domain. This will be a consequence in part of increasing connectivity via the Internet of Things (see Lanza et al 2015) and the fact that this connectivity will involve physical functions such as controlling vehicles and infrastructure. Key emerging challenges are identified as ensuring transparency, knowledge-exchange and coordination in research and action across mobility sectors, unimodal approaches represent a threat to security overall. Given that IM is data driven, data security represent an important emerging challenge in relation to: privacy of customers and companies; the security of Open Data; evolving legal requirements for personal data protection and commercial incentives to ensure protection of personal data (TSC 2016).

Understanding traveller attitudes to trade-offs between privacy and freedom on the one hand and security on the other has been an increasing focus of research in recent years (see McCarthy et al 2016a and 2016b; Patil et al 2014). However, the evidence base is limited at this stage. Developing knowledge in this area, including an appreciation of the diversity of perspectives and an associated population segmentation analysis (building on cluster analysis work by McCarthy et al 2016a and 2016b) represents an important challenge/opportunity in this research field.

Staff security training

Staff training and public awareness raising in relation to crisis management have been identified as important future challenges (EC 2017; Beecroft and Pangbourne 2015a). This relates to a wider challenge regarding the need to provide staff training which reflects changes in wider society to meet the requirements of changes in both demographic structure (particularly ageing societies, increasing urbanisation deriving in part from international migration and its associated ethnic and cultural diversity) and social behaviour. This also relates to the issue of how to best communicate security messages to passengers and develop a society-wide security culture (EC 2017). Developing such a culture represents a significant challenge going forward. Hoijtink (2015) investigated efforts to establish a common security culture in mass transportation and found that the culture was not stable and was difficult to enact due to *"the uneasy drawing together of transport operations and security objectives, terrorism and graffiti, and military and civil logics of security."* A further concern in this regard was identified by Carter et al (2016) that a culture of paranoia might be engendered and that passive forms of surveillance through sensor technology and video analytics were a preferable approach. The better utilisation of technology in training e.g. simulations, gaming and mobile apps was another identified challenge in this theme (EC 2017).

Passenger Security

A key emerging challenge in this theme is to apply the systematic approaches to design and evaluation of security measures common in aviation to all passenger modes. This relates particularly to threat detection and prevention and is inherently linked to developing scanning technologies and the collection and utilisation of passenger information: *"research is needed into how this information might be linked to other information, such as that available on social media, to potentially differentiate the security approach taken for different passengers."* (EC 2017). Linked to information concerns, Beecroft and Pangbourne (2015b) in the UK have identified concerns regarding the degree to which passenger information systems and services account for the personal security concerns of passengers. These relate particularly to the dynamic nature of personal security concerns associated with the impacts of journey disruption as well as temporal factors (see also Ceccato and Uittenbogaard 2014) and the differing requirements and perceptions of different travellers (e.g. gender, age, language, etc.). For example, a review of international research evidence on harassment on public transport and its impacts on women's travel behaviour by Gardner et al (2017) concluded that:

- Sexual harassment on public transport appears to be a growing issue, but understanding is frustrated by a lack of data and under-reporting;
- Harassment reinforces fear of crime, which limits womens mobility and reduces their use of public transport;
- Significant proportions of young women believe that it is unsafe to use public transport at night;
- Environmental interventions such as CCTV and lighting appear to have limited impacts on reducing fear, whilst formal surveillance through police or public transport employees is viewed more positively by passengers and has been proved effective;
- and 'soft measures' such as public awareness campaigns and improved reporting mechanisms are highly valued by women.

Masoumi and Fastenmeier (2016) in Germany identified knowledge gaps in public perceptions of security in public transport in relation to:

> *"the role of the size of urban population; differences between racial, religious, and sexual minorities and the majority of citizens; possible dissimilarities between different regions and sub-cultures; and the influence of micro-scale built environment, for instance in case of rail and bus stations and the surroundings."*

Such findings relate to a more fundamental concern identified in the research regarding the degree to which transport operators and service providers understand their customers and non-customers and their perceptions/needs in relation to security (see Beecroft and Pangbourne 2015b; Fyhri and Backer-Grøndahl 2012 and Roche-Cerasia et al 2013).

Beecroft and Pangbourne (2015a and 2015b) identified further challenges in the passenger security domain associated with trends towards the blurring of boundaries between traditional collective and private transport modes. This process is being accelerated by the growing market for shared mobility services. It is linked to current and potential future services and practices such as car sharing and connected and autonomous vehicles and is facilitated by ICTs such as mobile platforms and associated social media (see Hensher 2017; Docherty et al 2018; and Hannon et al 2016). Provision of such services generates a range of security questions associated with data integration and sharing (see Callegati et al 2016) as well as social and behavioural norms (see Merat et al 2017), which could be critical factors in the success of such services and the realisation of the MaaS business model.

Findings (3): What technologies are expected to have the biggest impact on security of transport in the future?

Before discussing the impacts of specific technologies it is important to acknowledge some general principles in the relationship between technology, transport and security. As Newton (2016) states: "The speed of change brought about by rapid developments in transport, combined with exponential advances of technology, result in a rapidly changing, dynamic and evolving landscape for transport-related crime opportunities." Critically, Newton states: "crime design is often an afterthought of new technology, and rarely built in at the outset of invention and or innovation of new technology." In this context, it is sensible to anticipate 'crime waves' to follow the introduction of transport technologies prior to reactive security measures being taken (Farrell et al 2011). This problem is predicted to be particularly acute in relation to cyber security threats to transport (TSC 2016). The criminal justice system also struggles to keep up with the pace of transport technology change. The challenge is therefore to introduce security considerations proactively at the design and early implementation phases on technological innovations.

When considering the relationship between transport technology and security it is important to remember that technology should not be used to replace people on grounds of security as people remain the most effective source of reassurance for passengers (Beecroft et al 2007; Delbosc and Currie 2012; Beecroft and Pangbourne 2015a, Carter et al 2016; McCarthy 2016a and 2016b; Newton 2016). This points to a significant danger when focussing upon technology in seeking to address transport security problems - the potential neglect of user needs, an example here might be the issue of target hardening increasing the severity of criminal activity e.g. biometric vehicle access may make the human being the target/weakest link in vehicle theft (Beecroft et al 2007). In considering how transport technologies influence crime opportunities Newton (2016) proposes five different interactions or impacts:

1. Transport technology dependent crime (transport system is target of crime e.g. hijacking, vehicle theft, fare evasion)
2. Transport technology as an enabler of crime (transport system as new arena for existing crime e.g. robbery, theft from person, assault,)
3. Transport technology as an enhancer of crime (transport technology increases scale/extent of crime e.g. theft of personal data on Wi-Fi networks or from payment cards, use of vehicles in theft, terrorist acts on transport networks)
4. Transport technology as a preventer of crime (transport technology reduces crime opportunities e.g. CCTV, scanning and access controls, cashless travel cards, ANPR)

5. Transport technology as an influence on perceptions of crime (transport technology positively influences travel perceptions and fear of crime e.g. real time information, help points, secure design, in-vehicle CCTV streaming)

Taking Newton's framework and drawing on wider evidence, a range of technologies that are likely to have the biggest impact on future security of transport are presented in **Table 1**. These technologies are grouped into Vehicle and ICT categories. The technologies chosen can only be illustrative given the complexity and sheer proliferation of new technologies that must be anticipated. These technologies have also been chosen to illustrate the range of potential impacts and the fact that they can be both positive and negative (all five interactions/impacts from Newton's framework are evident in both categories in **Table 1**). This dichotomy is key in highlighting risk and uncertainty which are critical issues when assessing potential impact. A significant casual factor of such uncertainty is that technology effects are not solely a consequence of what the technology is capable of but also of how it is used by people (Huber and Lyons 2013).

Some technologies designed specifically as transport security technologies (e.g. blast resistant materials, scanning and access control including biometrics) are not included as the degree of risk and uncertainty associated with their impacts is likely to be comparatively small. This is not to say that transport security technologies do not have the potential to cause negative security impacts. McCarthy et al (2016a and 2016b) investigated the attitudes to and risks associated with linking security technology and social networking apps in the form of personal security apps (which turn a smartphone into a type of panic alarm). They found that:

> *"security technologies could also pose their own risks with regard to transport users' privacy through the potential for data collection and storage. Transport, in particular, allows the data collector potential access to information on the users' habits through the location information that could be collected during an*

> *individual's interaction with technology during their travels."(McCarthy et al 2016b).*

Conclusion

This review has considered an extensive range of evidence in seeking to address the three research questions. In relation to current and emerging challenges, the challenges are many and varied. When looking across the five themes in our public transport security typology the following priority challenges can be determined:

What are the current security challenges for public transport networks?

- How do we enhance the security of our public transport networks, services and infrastructure (learning from aviation) without significant impacts upon convenience and privacy?
- How do we resolve interoperability and communication problems across our public transport systems to maximise the benefits of increasing connectivity?
- How do we realise the benefits of increasing connectivity in our public transport systems whilst mitigating the risks?
- How do ensure that the transport sector has the skills to mitigate the risks of a dynamic, complex and increasingly connected operating environment?

What are the emerging security challenges, looking out to 2040?

- How do we ensure security for users and service providers in a future mobility system which is data driven?
- How do we establish principles of systematic design and evaluation of security measures for all modes?

- Is transparency, knowledge-exchange and coordination achievable in research and action across mobility sectors to enhance security?
- How can we better understand people's behaviour, needs and attitudes in relation to travel, technology and security?

In relation to research question 3 the following key findings have been identified:

What technologies are expected to have the biggest impact on security of transport in the future?

Before assessing impact we need to recognise that the pace of change in transport and technology results in a rapidly changing, dynamic and evolving landscape for public transport-related crime. Crime prevention is often an afterthought of new technology design and so crime waves can often follow the introduction of transport technologies prior to reactive security measures being taken. Technology should not replace people on grounds of security as people remain the most effective source of reassurance for passengers.

The biggest impact technologies are grouped into categories of Vehicle (Unmanned Aerial Vehicles; Connected and Autonomous Vehicles and Electric Vehicles) and ICT (Internet of Things; social media; mobile platforms; Open Data, Big Data and 3DP). These technologies illustrate a wide range of potential impacts both positive and negative. This dichotomy is key in highlighting risk and uncertainty which are critical issues when assessing potential impact. In relation to ICTs, the biggest impacts relate to connectivity and data sharing and these represent both vulnerabilities and strengths. In relation to vehicle technologies, automation and connectivity are the factors most influencing impact for good or ill.

This review of security and future mobility has contributed to scholarly knowledge by highlighting significant current, emerging and potential future challenges. Lack of data and data reliability have been identified as common problems in the field of transport crime and security. Technology may address some of the technical data challenges, but the human dimension around reporting crime is a more difficult issue. Developing a more proactive, anticipatory approach to threats and challenges is critical and will require action across all three fields of public transport, security and technology. It will also depend upon better understanding the interfaces between these three fields. This understanding requires changes in managerial practice to improve communication between public transport stakeholders across these three fields and an associated collective recognition of their interdependence. This recognition must precede, not follow security challenges if a more secure future for mobility is to be achieved.

Disclosure statement

No potential conflict of interest was reported by the author

References

Azees, M; Vijayakumar, P. and Deborah, L. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, 10, 6, 379–388.

Beecroft, M; McDonald, M. and Voge, T. (2007). Achieving personal security in future domestic travel: technology and user needs. *IET Intelligent Transport Systems*, 1, 2, 69 –74.

Beecroft, M. and Pangbourne, K. (2015a). Future prospects for personal security in travel by public transport. *Transportation Planning and Technology*, 38, 1, 131–148.

Beecroft, M. and Pangbourne, K. (2015b). Personal security in travel by public transport: the role of traveller information and associated technologies. *IET Intelligent Transport Systems*, 9 2, 167–174.

Borjesson, M. (2012). Valuing perceived insecurity associated with use of and access to public transport. *Transport Policy*, 22, 1-10.

British Transport Police (2018) Statistical Bulletin 2017-18. Available, as at 28/6/19: https://www.btp.police.uk/about_us/your_right_to_information/publications.aspx

Callegati, F; Giallorenzo, S; Melis, A. and Prandini, M. (2016). Data security issues in MaaS-enabling platforms. IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI). Available (as at 11/12/17): http://ieeexplore.ieee.org/document/7740624/#full-text-section

Carter, E; Paragreen,J; Valfrè, G. and Fletcher, D. (2016). Passenger acceptance of counter-terrorism security measures in stations. *IET Intelligent Transport Systems*, 10, 1, 2–9.

Cavallini, S; D'Onofrio, F; Bouchon, S. and Giusto, C. (2014). Enhancing transport security: Characterization and identification of the main security challenges in 5 transport subsectors. 2014 IEEE International Carnahan Conference on Security Technology (ICCST). Available (as at 5/12/17): http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6987000

Ceccato, V. and Uittenbogaard, A. (2014) Space–Time Dynamics of Crime in Transport Nodes, *Annals of the Association of American Geographers*, 104:1,131-150

Cole, M and Kuhlmann, A. (2012). A scenario-based approach to airport security. *Futures*, 44, 319-327.

Delbosc, A. & Currie, G. 2012. Modelling the causes and impacts of personal safety perceptions on public transport ridership. *Transport Policy* 24: 302-309.

Docherty, I; Marsden, G. and Anable, J. (2018). The governance of smart mobility. *Transportation Research Part A*. 115: 114-125.

EC (2017). Research Theme Analysis Report: Transport Security. European Union. Available (as at 5/12/17): http://www.transport-research.info/sites/default/files/TRIP_Report_Transport_Security.pdf

Farrell, G; Tseloni, A. and Tilley, N. (2011). The effectiveness of vehicle security devices and their role in the crime drop. *Criminology & Criminal Justice*, 11(1) 21–35.

Fyhri, A. and Backer-Grøndahl, A. (2012). Personality and risk perception in transport. *Accident Analysis and Prevention*, 49, 470-475.

Gardner, N., Cui, J. and Coiacetto, E. (2017). Harassment on public transport and its impact on women's travel behaviour. *Australian Planner*, 54, 1, 8-15.

Hannon, E, McKerracher, C., Orlandi, I. and Ramkumar, S. (2016). An Integrated Perspective on the Future of Mobility. McKinsey Report. Available (as at 11/12/17): https://www.mckinsey.com/business-functions/sustainability-and-resource-productivity/our-insights/an-integrated-perspective-on-the-future-of-mobility

Hensher, D. (2017). Future bus transport contracts under a mobility as a service (MaaS) regime in the digital age: Are they likely to change? *Transportation Research Part A*, 98, 86-96.

Hoijtink, M. (2015). Performativity and the project: enacting urban transport security in Europe. *Critical Studies on Terrorism*, 8:1, 130-146.

Holgersson, A. and Björnstig, U. (2014). Mass-casualty attacks on public transportation. *Journal of Transportation Security*, 7, 1-16.

Holtrop, D. and Kretz, D. 2008, Research security & safety: an inventory of policy, legislation and regulations (in Dutch). Research Report 141223/EA8/043/000603/sfo. The Netherlands: Arcadis.

Hubers, C. and Lyons, G. (2013). Assessing future travel demand: a need to account for non-transport technologies? *Foresight: the Journal of Futures Studies, Strategic Thinking and Policy*; 15, 3, 211-227.

Javed, M; Hamida E. and Znaidi, W. (2016). Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors,* 16, 6, 879, 1-25.

Lanza, J., Sánchez, L., Muñoz, L., Galache, J.A., Sotres, P., Santana, J.R. and Gutiérrez, V. (2015). Large-Scale Mobile Sensing Enabled Internet-of-Things Testbed for Smart City Services. International Journal of Distributed Sensor Networks vol. 2015, Article ID 785061, 15 pages, 2015. Available (as at 5/12/17): http://journals.sagepub.com/doi/pdf/10.1155/2015/785061 .

Levine, N. and M. Wachs, (1986). Bus Crime In Los Angeles I – Measuring the Impact." *Transportation Research A*, 20, 4, 273-284.

McCarthy, O; Caulfield, B. and O'Mahony, M. (2016a). How transport users perceive personal safety apps. *Transportation Research Part F*, 43, 166-182.

McCarthy, O; Caulfield, B. and O'Mahony, M. (2016b). Technology engagement and privacy: A cluster analysis of reported social network use among transport survey respondents. *Transportation Research Part C*, 63, 195-206.

Masoumi, H. and Fastenmeier, W. (2016). Perceptions of security in public transport systems of Germany: prospects for future research. *Journal of Transportation Security*, 9, 105-116.

Merat, N; Madigan, R. and Nordhoff, S. (2017). Human Factors, User Requirements, and User Acceptance of Ride-Sharing in Automated Vehicles. International Transport Form Discussion

Paper 2017-10. Available (as at 11/12/17): https://www.itf-oecd.org/sites/default/files/docs/human-factors-ride-sharing-automated-vehicles_0.pdf

Newton A (2004) Crime on Public Transport: 'Static' and 'Non-Static' (Moving) Crime Events. *Western Criminology Review*, 5, 3, 25-42.

Newton, A. (2016) 'Crime, Transport and Technology'. In: *The Routledge Handbook of Technology, Crime and Justice*. London, UK: Routledge. pp. 281-294. ISBN 9781138820135

OED Online. (2017). Search result for definition of security. Available (as at 7/12/17): http://www.oed.com/view/Entry/174661?redirectedFrom=security#eid

Patil, S; Potoglou, D; Lua, H; Robinson, N. and Burge, P. (2014). Trade-off across privacy, security and surveillance in the case of metro travel in Europe. *Transportation Research Procedia*, 1, 121 – 132.

Petit, J. and Shladover, S. (2015). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems,* 16, 2, 546-556.

Reggiani, A. (2013). Network resilience for transport security: Some methodological considerations. *Transport Policy*, 28, 63-68.

Reniers, G. and Amyotte, P. (2012). Prevention in the chemical and process industries: Future directions. *Journal of Loss Prevention in the Process Industries,* 25, 1, 227-231.

Roche-Cerasia, I: Rundmo, T; Foss Sigurdson, J. and Moe, D. (2013). Transport mode preferences, risk perception and worry in a Norwegian urban population. *Accident Analysis and Prevention*, 50, 698-704.

Steenbruggen, J; Borzacchiello, M; Nijkamp, P. and Scholten, H. (2013). Data from telecommunication networks for incident management: An exploratory review on transport safety and security. *Transport Policy*, 28, 86-102.

Szyliowicz, J. (2013). Safeguarding critical transportation infrastructure: The US case. *Transport Policy*, 28, 69-74.

TSC (2016). Cybersecurity and Intelligent Mobility. Transport Systems Catapult. Available (as at 5/12/17): https://s3-eu-west-1.amazonaws.com/media.ts.catapult/wp-content/uploads/2016/11/24133246/3416_Cyber-Security_Report_Final-1.pdf

Zamparini, L. and Shiftan, Y. (2013). Editorial: Special Issue—"Transport security: Theoretical frameworks and empirical applications". Selected papers from the first joint meeting of the Network on European Communication Transport Activity Research (NECTAR) Cluster 7 on Transport and Security and the World Conference on Transportation Research (WCTR) Special Interest Group (SIG) 14 on Transport Security. *Transport Policy*, 28, 61-62.

Transport technology	**Transport technology dependent crime**	**Transport technology as an enabler of crime**	**Transport technology as an enhancer of crime**	**Transport technology as a preventer of crime**	**Transport technology as an influence on perceptions of crime**
Vehicles technologies: Unmanned Aerial Vehicles (UAVs) Connected and Autonomous Vehicles (CAVs) Electric Vehicles (EVs)	UAV/CAV Hijack/hacking at varying scales (including fleets) Theft of data (vehicle, network and personal) from vehicle and/or associated infrastructure Theft/misuse of associated charging infrastructure and vehicle batteries for EVs	UAV/CAV provide new transport arena for crime (driverless = anonymous) e.g. cargo and data theft, terrorism, etc.	Deployment of UAVs/CAVs in existing transport environments to extend scale and extent of threats e.g. terrorism, cargo and data theft, etc. CAV access controls increase severity of vehicle theft/hijack as human is weak link.	UAV surveillance for threat detection and deployment for crisis management and in hazardous environments. CAV access controls reduce incidence of vehicle theft. CAVs for potential passive surveillance and monitoring on transport network.	UAV as visible monitoring reassurance akin to CCTV CAVs viewed as safe and secure alternative to collective modes. CAVs secure travel environment encourages travel by non-drivers.

Information and Communication technologies: Internet of Things Social media Mobile platforms Open Data Big Data	Connectivity and ICT dependency of transport networks and associated critical infrastructure generates opportunities for large scale impacts of cyberattacks (both external hacking and 'insider' threats).	New transport-based and relatively unsecure public arena for digital crime e.g. data theft, ID theft, fraud, malware/ransomware, etc. Individual risk heightened by data collection, retention and sharing processes inherent in personalised mobility services such as MaaS (user profiling over time).	Cascade effects of ICT deployment to generate threats and inhibit crisis management e.g. mobile network overload, social media misuse, distributed denial of service, etc.	Effective networks for anonymised journey planning and payment offer potentially more secure travel e.g. use of distributed ledger and cryptocurrency technologies	Enhanced (dynamic, accurate, ubiquitous) information provision and communication (via staff and through digital platforms) are key source of traveller reassurance, confidence and control over journey. Passive monitoring of travel behaviour through mobile applications may provide reassurance to travellers.

Table 1 New transport technologies and their potential security impacts.