Lewle Sebastian Seneviratne

University of Essex

Research Methods and Professional Practice

Unit 7:

Implementing Cyber Security tools and/or techniques in local road and railway transportation system in Denmark

LITERATURE REVIEW

Introduction

Nowadays, transportation infrastructure continues to extend from isolated nodes to extensive, connected networks enabling intelligent and digitalised public transport. Consequently, cybersecurity is a critical concern, as merging cyber threats will impact the transport service operations and the entire economy and potentially the health and safety of residents (European Union Agency for Network and Information Security, 2015; Ministry of Transport, 2019a).

Literature review focuses on technologies deployed in Denmark and covers current technologies and the technologies known to be considered for future deployment in road and railway transportation infrastructure. A review of Danish authorities' existing reports compiles current transportation system deployment with increased dependence on digital solutions (Ministry of Transport, 2019b) and the efficiency of transport services based on time-critical, complex IT systems directly depends on cybersecurity (Mecheva & Kakanakov, 2020; Pizzi, 2020).

Existing reports have focused on threat assessment and implementation of effective cybersecurity policies and practices in public transportation management (European Union Agency for Network and Information Security, 2015; Center for Cyber Security, 2021a; Center for Cyber Security, 2021b). In order to investigate effective cyber security techniques and tools, the literature review takes a technical approach and evaluates the current public transit technologies and their vulnerabilities by reviewing known vulnerabilities discussed in a variety of technical venues and assessing the security considerations.

Background

The transportation subsystem is under the authority of the Ministry of Transport, which is responsible for the sector in general and comprises railway, aviation, roads, and maritime ports. Figure 1 represents the current organisational structure of the Ministry of Transport, Denmark.

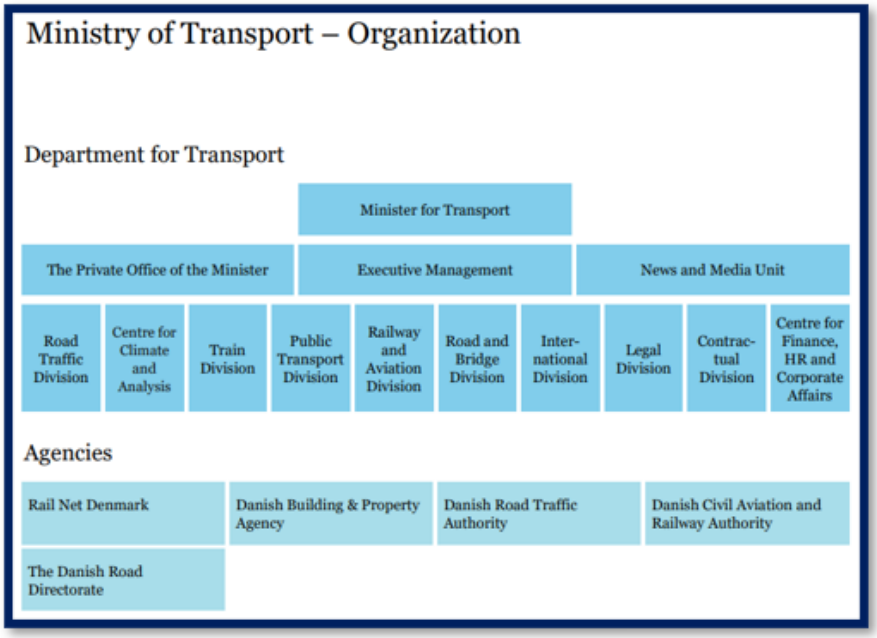

Figure 1: Ministry of Transport – Organization (Ministry of Transport, 2022)

Today, Danish transportation systems have enhanced their operations and financial transactions and services with the deployment of modern technologies, such as passenger counters, autonomous vehicle location, traffic signal control systems, connected and autonomous vehicles (CAVs), and other mobile applications (Ministry of Transport, 2019b). The achieved advantages, such as increased ridership and rider satisfaction, improved fleet management and easily accessible fare payments, highlight the continued growth in transportation technologies in recent years (Ministry of Transport, Building, and Housing, 2017; Brakewood et al., 2018).

However, in 2018, Danish public transport provider DSB's ticket systems and website were hit by a distributed denial of service attack, and for hours, travellers could not buy tickets neither via DSB's app, their website, nor at ticket machines (Valeur, 2018). The cyber-attacks thus showed that the technological threat can become an expensive affair for the Danish transportation system and its vendors and that hackers can hit government institutions that are absolutely vital for maintaining a well-functioning society.

Therefore, it is crucial to understand evolving vulnerabilities and learn effective mitigation strategies as the transportation sector is a notably attractive target for rivals seeking a broad impact area, such as extorting finances from private corporations and public authorities, disrupting transport sector operations, sabotaging consumer confidence (Center for Cyber Security, 2021a).

Transit Technologies

The section reviews current transportation technologies with a focus on cybersecurity.

Mobility as a Service (MaaS)

MaaS, integrates diverse transport services into a single service provider with on-demand accessibility. It works as a service model by placing the rider in the centre and framing the mobility system around the rider's choices while allowing them to plan, book and pay for their trips simultaneously (Ho et al., 2018; Hensher & Mulley, 2021; Zhao et al., 2021).

Interconnectivity between different transport modes and service providers, rider-needs-based, and service-bundling can be highlighted as the main characteristics of

a personalised mobility package offered through MaaS (Jittrapirom et al., 2017). Today, in modern intermodal intersections, diverse transit modes are available to switch from private transport to public, such as Park&Ride and Bike&Ride facilities (Heinrich-Böll-Stiftung European Union, 2021). These initiatives can develop better and enhance traffic management. Thus, MaaS aims to facilitate seamless multimodal travel to provide a sustainable alternative to using its own private transportation solutions (Hensher & Mulley, 2021; Zhao et al., 2021). Figure 2 represents the seamless links between various public transport in Helsinki, with an overarching digital approach.

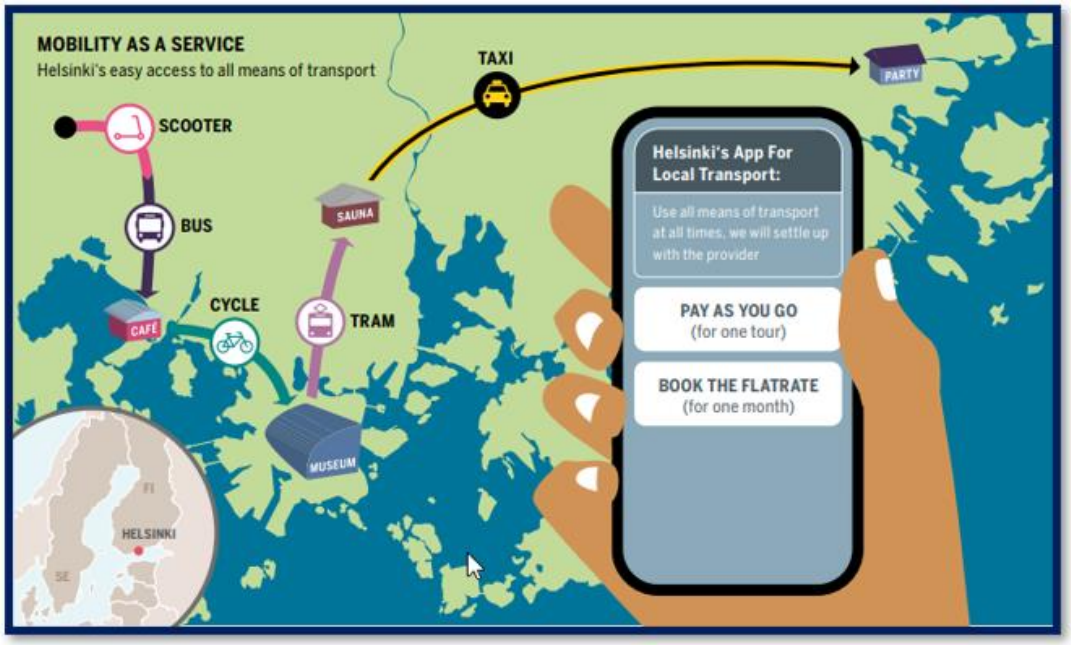

Figure 2: Mobility as a Service (MaaS): Helsinki's App for Local Transport (Heinrich-Böll-Stiftung European Union; 2021:35)

Digitalisation is a critical success factor for all transit solutions. Riders can effortlessly access multimodal mobility on digital platforms for online trip planners, real-time rider information, and e-ticketing, making mobility handling more manageable (Bieser & Kriukelyte, 2021). The use of Artificial Intelligence (AI) also helps prevent congestion. By analysing anonymised location data from mobile-based probe detectors and taxi

GPS positioning-based detectors, it is possible to anticipate traffic flows and design better urban spaces and infrastructure (Xing et al., 2022). At the same time the anonymised location data may serve as an influential basis for real-time rider information, such as route guidance (Tettamanti & Varga, 2014; Fekih et al., 2021).

Denmark has also promoted MaaS. Based on the original national multi-modal journal planner, a new pilot MaaS service Rejseplan was launched in May 2018, developed by the transport authority to connect public transport to other private services. Rejseplan integrates regular bus services with Flextur (bus service for seniors started in 2003), a rural only feeder taxi service Plustur, and GoMore (a carpooling service). In addition to conventional public transport, a MaaS based Flextrafik was introduced to meet the health care and social transport needs (Leung et al., 2021).

Figure 3 represents the Rejseplan App which can integrated intoconventional public transport trip.

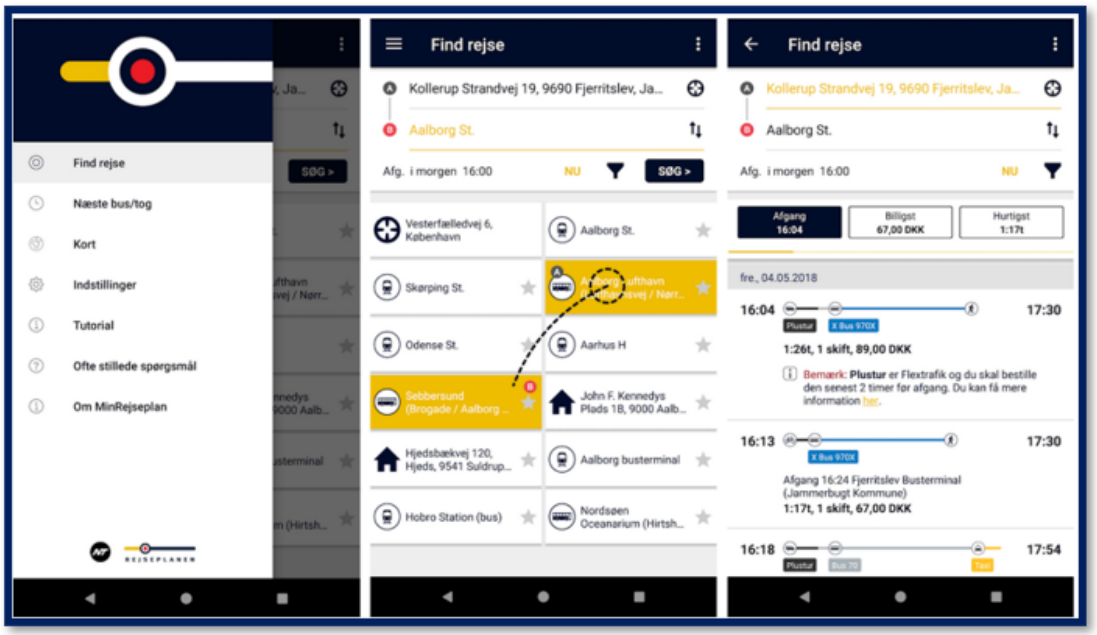

Figure 3: Rejseplan App which can integrated intoconventional public transport trip (Leung et al.; 2021:18)

In 2018, the launch of the Danish Easier Public Transport policy included several digital mobility initiatives to encourage planning, payment and ticketing sharing between private and public transportation modes (Ministry of Finance and Ministry of Industry, Business and Financial Affairs, 2019).

Security Consideration

Data-driven services intrinsically carry cybersecurity concerns, such as ownership of data? What constitutes ethical and appropriate use of data? Should user data be automatically shared, or should it need careful consideration regarding what, why, with whom, when and how data sharing before an incident relates to law enforcement and emergency services or for specific purposes, such as managing crises?

A more realistic threat is an attacker gaining access to the GPS positioning of vehicles which represents a risk to privacy and can allow competitors or other entities to reliably map the routes and transportation movements (Mecheva & Kakanakov, 2020). It could also be that the right combination of user-specific data and transport choices to fit the multimodal transport offering may mean a compromise must be made between user-data sharing and data protection on occasions such as during pandemics (The Global Infrastructure Hub, 2020).

One of the key enablers of the MaaS ecosystem is the exploitation of data using predictive AI models. However, it has been widely accepted that AI algorithms can be exploited by malicious actors using sophisticated cyber-attacks (Dixon & Eagan, 2019; Truong & Zelinka, 2019; Guembe et al., 2022).

An initiative focusing on better utilisation of mobile phones' location data will uphold Denmark as a data-ethical frontrunner. At the same time, it promotes the development of new innovative databased technologies in collaboration with the

telecommunications industry. The pilot project aims to deliver clarity to the legal and data-ethical frameworks of exhibiting and utilising location data while it tests the commercial prospects of utilising location data for AI (Ministry of Finance and Ministry of Industry, Business and Financial Affairs, 2019).

In addition, the project trials aim to identify aggregation levels of data that secure the individuals' anonymity while fostering the development of smart resolutions to benefit citizens, businesses and authorities (Ministry of Finance and Ministry of Industry, Business and Financial Affairs, 2019).

Traffic Signal Controllers and Traffic Signal Preemption/Priority

Traffic signal control systems have grown from standalone pieces of technology harmonised through synchronised time clocks to sophisticated programs operating on a complex networked system of systems consisting of various sensors, controllers, malfunction management units, and communication devices (Hou et al., 2022). Today, a wealth of data accessible to traffic signal controllers through connected, intelligent transport systems is also useful for integrating existing traffic signal control systems in urban environment planning (Rafter, 2020). This transition significantly improves citizens’ quality of life by optimising the time through smooth network-wide traffic flows and reduction in exhaust emission pollution (Li et al., 2016). Figure 4 represents the main components of a traffic signal system.

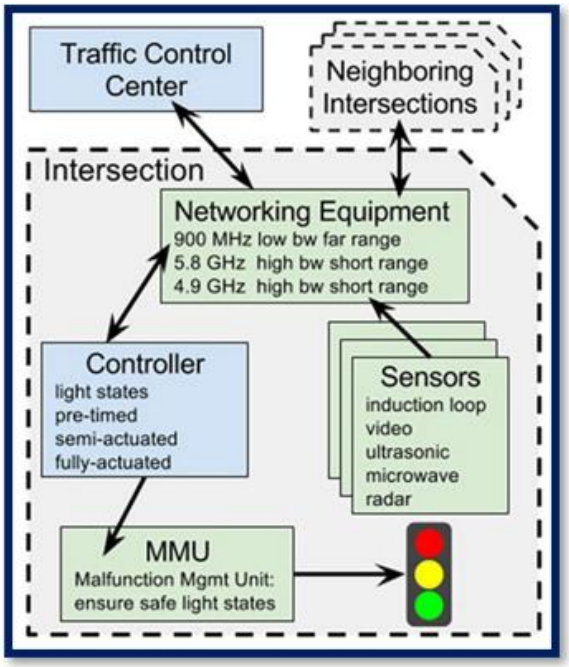

Figure 4: Main components of a traffic signal system (Li et al.; 2016)

Security Consideration

Security researchers have shown that advanced cyber-physical traffic signal systems have many weaknesses that could be easily exploited, letting an attacker directly adjust traffic signal indications using surprisingly inexpensive techniques (Ghena et al., 2014; Li et al., 2016; Chandran et al, 2017; Hou et al., 2022).

For example, Ghena et al. (2014), by analysing a wireless traffic signal system security, uncovered vulnerabilities such as a lack of standard security procedure (i.e. unchanged the default usernames and passwords, open debug ports) and lack of encryption support in the wireless communication. Figure 5 represents some of the identified cybersecurity vulnerabilities in traffic signal systems.

Classification	Attack techniques	Consequences/use cases
Cyberattack on traffic controller [34, 35]	password cracking, social engineering to acquire device	control traffic signal, send commands to the controller
Cyberattack by sniffing [29, 30]	sniffing sensor identification information, commands, etc.	send falsifying commands and data, manipulation of devices
Cyberattack on traffic sensor [35, 36]	wireless sensors spoofing	destabilize the traffic network
Physical attack on traffic controller [35]	Sabotaging physical networking components	affect performance, availability of devices or services
Cyberattack on traffic controller [37]	denial-of-service attack	take down the network to which the traffic signal is connected
Cyberattack on traffic sensor [38]	data spoofing, masquerade as connected vehicles to send data	influence the signal control algorithms by sending invalid data

Figure 5: Cybersecurity vulnerabilities in traffic signal systems (Hou et al.; 2022).

Maliciously manipulating traffic control systems to satisfy personal demands or impair public safety would no longer occur just in Hollywood films but also potentially in real life as traffic intersection and sign management systems are likely to be prime targets if plans, devices, and protocols are not highly safeguarded (Hou et al., 2022).

Though it is vital to have real-time data availability in traffic management, protecting data and controlling access to have data available only to those who need it, is crucial to move forward with connected and more advanced systems.

Connected and Autonomous Vehicles (CAVs)

Integrating diverse technologies, connected and autonomous vehicles (CAVs) have continued to anticipate enhanced transportation efficiency, reduction in accidents, and improved safety while offering excellent mobility service options with ease of environmental damage. The CAVs paradigm will continue to unfold steadily and

progressively throughout the 2020s and the future, with increased infrastructure and communication technologies improvements (Rios-Torres & Malikopoulos, 2016; Clements & Kockelman, 2017; Fu et al., 2020; Liu et al., 2020; Sun et al., 2021).

CAVs have also been deployed in Denmark. While Denmark's Metroselskabet continues to use new autonomous trains from Hitachi Rail Italy (HRI) to expand Copenhagen Metro, Copenhagen is looking forward to experiencing a self-driving electric shuttles service as part of EU-funded research projects (AVENUE and LINC), which combines intelligent autonomous technology and sustainable urban planning (Railway Technology, 2018: Connectedautomateddriving.eu, 2020; EU Commission, 2020).

Security Consideration

Security is a critical challenge in the era of CAVs technology, as autonomous technology makes it possible for remote attackers to hack into CAVs and be used to commit crimes, anonymising the offender (Newton, 2016; Parkinson et al., 2017). Any failure of CAVs may result in severe loss of data privacy and may negatively impact vehicle safety or even cause accidents (Liu et al., 2020; Sun et al., 2021). A myriad of heterogeneous cyber and physical components of CAVs also present additional security challenges as the complex interactions between these components inside the CAVs make it challenging to model the system and the adversary (Rana & Hossain, 2021). Figure 6 represents the framework of CAVs in 6G Communications.

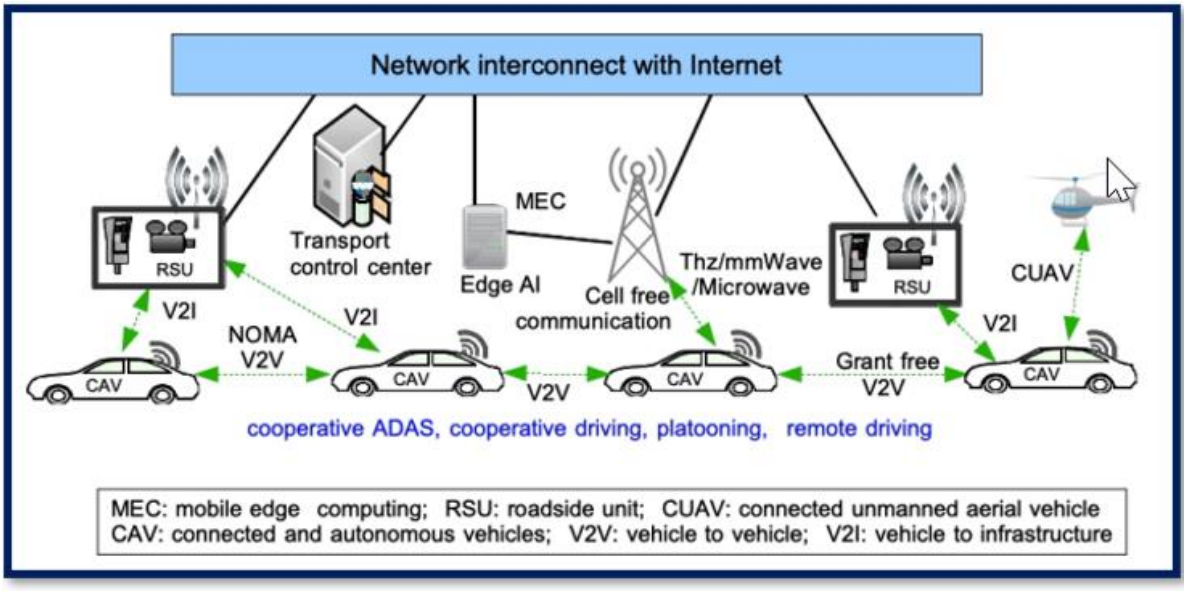

Figure 6: The framework of CAVs in 6G Communications (He et al.; 2020:5).

To make the matter worse, CAVs from different manufacturers are likely to have different architectures and components, making the modelling task even more challenging. The inertia of the physical components implies that a CAV cannot be easily stopped when under an attack (Sun et al., 2021). Therefore, a successful CAV system needs to respond and adapt to new security threats (even unknown zero-day threats) while guaranteeing operation safety in real-time. Figure 7 represents the potential attack surfaces in connected and autonomous vehicles based on a survey on the cyber security of CAVs.

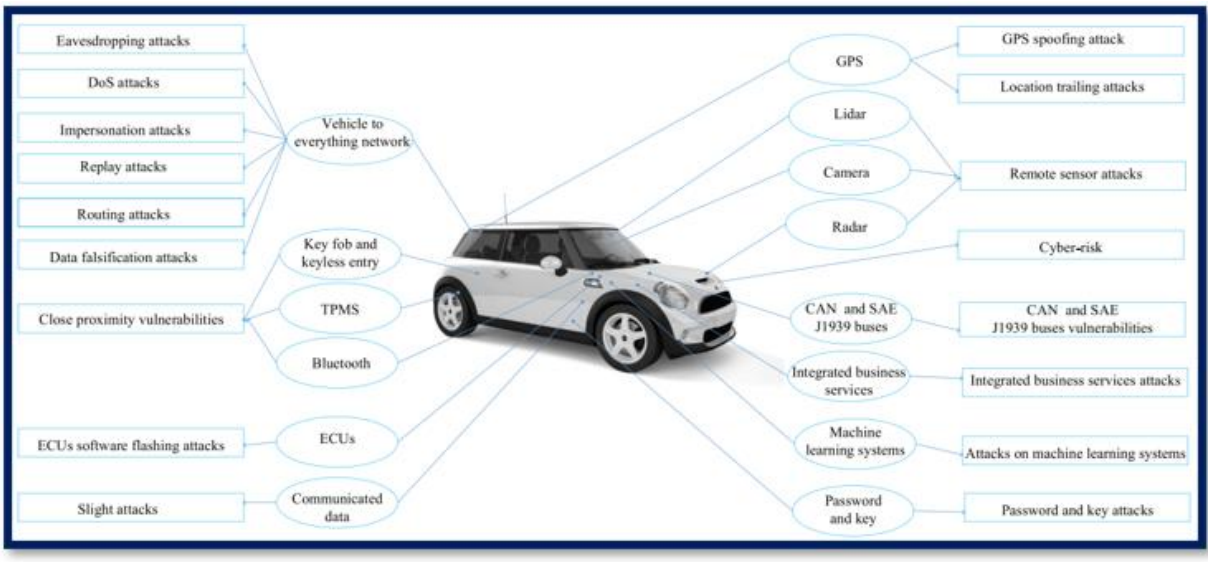

Figure 7: The potential attack surfaces in connected and autonomous vehicles. (Sun et al.; 2021:5).

According to Parkinson et al. (2017), a substantial portion of the identified research details, a reactive action to detect a cyber security vulnerability. However, the recent research by Meyer et al. (2021) forecasting the effects of the CAVs expansion on the cybersecurity of the transport system concluded that spending resources on CVAs cybersecurity would increase the degree of difficulty for conducting cyber-attacks. Consequently, the greater difficulty would discourage some would-be attackers and intimidate other would-be attackers unsuccessful in their endeavours.

Further, considering the environment of CAVs, it is vital that key stakeholders (i.e. the CAV manufacturers, intelligence providers, governments, regulators and consumers) thoroughly comprehend the prospects and liabilities associated with CAVs and work together proactively, sharing accountabilities rather than rationing flaws to one another (Liu et al., 2020; Sun et al., 2021).

Conclusion

In the mobility and transportation arena, cyber security is crucial to ensure responsible technological development and the use of data. As many auto manufactures, intelligence providers and governments accelerating toward a world of shared data-driven and autonomous mobility, consumers are approaching the prospect of technological development and use of data with caution (Pangbourne et al., 2020). Without guaranteeing safety and secure functioning of transportation, those investments could be for nothing (Nash et al., 2017).

By taking the hard-earned lessons learned from previous incidents in other countries and utilising focus-driven research, Denmark's transport ecosystem can keep itself ahead of cyber security challenges by adapting appropriate proactive safety measures and practical and robust cyber security solutions.

Furthermore, over the years, Denmark has managed to preserve high confidence in the public sector from both individuals and the enterprise society, which the government is looking forward to increasing to 90% from 83% before 2024 (Ministry of Finance and Ministry of Industry, Business and Financial Affairs, 2019).

Realising this goal and the potential in data sharing requires a common ethical basis for developing and using data and new technologies, which will continue to sustain confidence in work on data and new technologies. Thus, any development and use of data and technology must be within the relevant legislative framework, where the use of personal data should be still respected.

Reference List

Bieser, J. C. T. & Kriukelyte, E. (2021) T*he digitalization of passenger transport.* Available from: https://www.sams.kth.se/polopoly_fs/1.1124174.1638277889!/Bieser%20and%20Kriukelyte_Digitalization%20of%20passenger%20transport.pdf [Accessed 22 April 2022].

Brakewood, C., Macfarlane, G. & Watkins, K. (2015) The impact of real-time information on bus ridership in New York City. *Transportation Research Part C: Emerging Technologies* 53. DOI: 10.1016/j.trc.2015.01.021.

Brakewood. C & Watkins, K. (2018) A literature review of the passenger benefits of real-time transit information. *Transport Reviews* 39(3): 327–356. DOI: https://doi.org/10.1080/01441647.2018.1472147

Chandran, D., Zhang, Y. & Cheng, L. (2017) *A Survey on Cybersecurity of traffic signal systems*. Available from: https://www.researchgate.net/publication/328018680_A_Survey_on_Cybersecurity_of_traffic_signal_systems [Accessed 2 April 2022].

Connectedautomateddriving.eu (Jul 15, 2020) Testing autonomous mobility solutions in Copenhagen. Available from: https://www.connectedautomateddriving.eu/blog/testing-autonomous-mobility-solutions-in-copenhagen/ [Accessed 2 April 2022].

Clements, L. M. & Kockelman, K. M. (2017) Economic effects of automated vehicles. *SAGE Journals* 2606 (1): 106-114. DOI: 10.3141/2606-14

Center for Cyber Security (2021a) *The cyber threat against land and air transport*. Available from: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-for-land--and-air-transportation.pdf [Accessed 2 April 2022].

Center for Cyber Security (2021b) *The cyber threat against the Danish aviation sector*. Available from: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-threat-assessment-for-aviation.pdf [Accessed 2 April 2022].

Dixon, W. & Eagan, N. (Jun 19, 2019) 3 ways AI will change the nature of cyber attacks. *World Economic Forum*. Available from: https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/ [Accessed 22 April 2022].

EU Commission (Dec 16, 2020) LINC: Denmark to test driverless, electric buses for greener urban mobility. Available from: https://ec.europa.eu/regional_policy/en/projects/Denmark/linc-denmark-to-test-driverless-electric-buses-for-greener-urban-mobility#:~:text=Autonomous%20shuttle%20buses%2C%20each%20carrying,more%20than%20500%20dedicated%20users [Accessed 2 April 2022].

European Union Agency for Network and Information Security (2015) *Cyber Security and Resilience of Intelligent Public Transport - Good practices and recommendations*. Available from: https://www.enisa.europa.eu/publications/good-practices-recommendations [Accessed 2 April 2022].

Fekih, M., Bonnetain, L., Furno, A. & Bonnel, P. (2021) Potential of cellular signaling data for time-of-day estimation and spatial classification of travel demand: a large-scale comparative study with travel survey and land use data. *Transportation Letters The International Journal of Transportation Research*. DOI: 10.1080/19427867.2021.1945854

Fu, Y. et al. (2020) Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles. *IEEE Wireless Communications* 27(2): 197–203. DOI: 10.1109/MNET.001.1900310

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., & Halderman, J. A. (2014). *Green Lights Forever: Analyzing the Security of Traffic Infrastructure*. Available from: https://www.semanticscholar.org/paper/Green-Lights-Forever%3A-Analyzing-the-Security-of-Ghena-Beyer/7cdce6f75c8f1c5fd9d046b6c9424a11ec34d16a [Accessed 2 April 2022].

Guembe, B., Misra, S., Osamor, V. C. & Azeta, A. (2022) The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*. DOI: 10.1080/08839514.2022.2037254

He, J., Yang, K. & Chen, H. (2020) 6G Cellular Networks and Connected Autonomous Vehicles. *IEEE Network* 99: 1–7. DOI: 10.1109/MNET.011.2000541

Hensher, D. A. & Mulley, C. (2021) Mobility bundling and cultural tribalism -Might passenger mobility plans through MaaS remain niche or are they truly scalable? *Transport Policy* 100: 172–175. DOI: 10.1016/j.tranpol.2020.11.003

Heinrich-Böll-Stiftung European Union (2021) *The European mobility atlas*. Available from: https://eu.boell.org/sites/default/files/2021-07/EUMobilityatlas2021_2ndedition_FINAL_WEB.pdf [Accessed 2 April 2022].

Ho, C., Hensher, D. A., Mulley, C. & Wong, Y. Z. (2018) Potential uptake and willingness-to-pay for Mobility as a Service (MaaS): A stated choice study. *Transportation Research Part A* 117: 302–318. DOI: 10.1016/j.tra.2018.08.025

Hou, Y., Collins, K. & Van Wart, M. (2022) 'Intersection Management, Cybersecurity, and Local Government: ITS Applications, Critical Issues, and Regulatory Schemes', in: Sarwat et al. (eds.) *Smart Mobility - Recent Advances, New Perspectives and Applications [Working Title]*, London: IntechOpen. DOI: 10.5772/intechopen.101815

Jittrapirom, P., Feneri, A. M., Ebrahimigharehbaghi, S., Caiati, V., Narayan, J. & Gonzalez, M. J. A. (2017) Mobility as a Service: A Critical Review of Definitions, Assessments of Schemes, and Key Challenges. *Urban Planning* 2(2). DOI: 10.17645/up.v2i2.931

Leung, A., Burke, M., Akbar, D. & Kaufman, B. (2021) *Mobility as a Service Regional Research*. Available from: https://www.griffith.edu.au/__data/assets/pdf_file/0040/1379947/MaaS_Regional_Research_Report_FINALREPORT_Final1.pdf [Accessed 22 April 2022].

Li, Z., Jin, D., Hannon, C., Shahidehpour, M. & Wang, J. (2016) Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Physical Systems: Theory & Applications* 1(1):60-69. DOI: 10.1049/iet-cps.2016.0017

Liu, N., Nikitas, A. & Parkinson, S. (2020) Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology and Behaviour* 75: 66–85. DOI: 10.1016/j.trf.2020.09.019

Mecheva, T. & Kakanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems. *Computers* 9(4). DOI: https://doi.org/10.3390/computers9040083.

Meyer, S. F., Elvik, R. & Johnsson, E. (2021) Risk analysis for forecasting cyberattacks against connected and autonomous vehicles. *IEEE Journal of Transportation Security* 14: 227–247. Available from: https://link.springer.com/article/10.1007/s12198-021-00236-4 [Accessed 2 April 2022].

Ministry of Finance and Ministry of Industry, Business and Financial Affairs (2019) *National Strategy for Artificial Intelligence*. Available from: https://en.digst.dk/media/19337/305755_gb_version_final-a.pdf [Accessed 2 April 2022].

Ministry of Transport (2019a) Ny strategi for cyber- og informationssikkerhed. Available from: https://www.trm.dk/nyheder/2019/ny-strategi-for-cyber-og-informationssikkerhed [Accessed 2 April 2022].

Ministry of Transport (2019b) *Strategi for cyber- og informationssikkerhed 2019-2021 i transportsektoren*. Available from: https://www.trm.dk/publikationer/2019/strategi-for-cyber-og-informationssikkerhed-2019-2021-i-transportsektoren [Accessed 2 April 2022].

Ministry of Transport (2022) *Organisationplan for Transportministeriet*. Available from: https://www.trm.dk/media/oqxlpvvw/ministry-of-transport-organization-januar-2022.pdf [Accessed 2 April 2022].

Ministry of Transport, Building, and Housing (2017) *Reorganisation of the s-bane for driverless operation*. Available from: https://www.trm.dk/media/5oidavkw/final-report.pdf [Accessed 2 April 2022].

Nash, L., Wireman, M., Boehmer, G. & Hillaker, A. (2017) *Securing the future of mobility - Addressing cyber risk in self-driving cars and beyond*. Available from: https://www2.deloitte.com/uk/en/insights/focus/future-of-mobility/cybersecurity-challenges-connected-car-security.html [Accessed 2 April 2022].

Newton, A. (2016) 'Crime, transport and technology', in: McGuire, M. R. & Holt, T.J. (eds) *The Routledge Handbook of Technology, Crime and Justice,* London: Routledge.

Pangbourne, K., Mladenović, M. N., Stead, D. & Milakis, D. (2020) Questioning mobility as a service: Unanticipated implications for society and governance. *Transportation Research Part A: Policy and Practice* 131: 35-49. DOI: 10.1016/j.tra.2019.09.033.

Parkinson, S. et al. (2017) Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems* 18(11): 1–18. DOI: 10.1109/TITS.2017.2665968

Pizzi, G. (2020) Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment. *Transportation Research Procedia 45*: 250-257. DOI: 10.1016/j.trpro.2020.03.014

Rafter, C. B. (2020) *Integrating Connected Vehicles into Urban Traffic Management Systems*. Available from: https://eprints.soton.ac.uk/448150/1/craig_rafter_phd_ethesis_final.pdf [Accessed 22 April 2022].

Railway Technology (Mar 15, 2018) Hitachi to supply driverless trains for Copenhagen Metro. Available from: https://www.railway-technology.com/news/hitachi-supply-driverless-trains-copenhagen-metro/ [Accessed 2 April 2022].

Rana, M. & Hossain, K. (2021) Connected and Autonomous Vehicles and Infrastructures: A Literature Review. *International Journal of Pavement Research and Technology*. DOI: doi.org/10.1007/s42947-021-00130-1

Rios-Torres, J. & Malikopoulos, A. A. (2016) A survey on the coordination of connected and automated vehicles at intersections and merging at highway on-ramps. *IEEE Transactions on Intelligent Transportation Systems*18(5): 1066-1077. DOI: 10.1109/TITS.2016.2600504

Sun, X., Yu, R. F. & Zhang, P. (2021) A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems* 14: 1–20. DOI: 10.1109/TITS.2021.3085297

Tettamanti, T. & Varga, I. (2014) *Mobile Phone Location Area Based Traffic Flow Estimation in Urban Road Traffic*. Available from: https://www.researchgate.net/publication/260297863_Mobile_Phone_Location_Area_Based_Traffic_Flow_Estimation_in_Urban_Road_Traffic [Accessed 12 April 2022].

Truong, T. C. & Zelinka, I. (2019) A survey on artificial intelligence in malware as next-generation threats. *Mendel* 25(2):27-34. DOI: 10.13164/mendel.2019.2.027.

The Global Infrastructure Hub (GI Hub) (2020) *Mobility as a Service*. Available from: https://www.gihub.org/infrastructure-technology-use-cases/case-studies/mobility-as-a-service/ [Accessed 22 April 2022].

Valeur, J. (May 14, 2018) Sådan blev DSB's billetsystemer lagt ned: DDoS-angreb er internettets brostenskast. *Politiken*. Available from: https://politiken.dk/viden/Tech/art6510622/DDoS-angreb-er-internettets-brostenskast [Accessed 2 April 2022].

Xing, J., Cheng, Q., Wu, W. & Liu, R. (2022) Traffic State Estimation of Urban Road Networks by Multi-source Data Fusion: Review and New Insights. *Physica A: Statistical Mechanics and its Applications* 595. DOI: 10.1016/j.physa.2022.127079

Zhao, X., Andruetto, C., Vaddadi, B. & Pernestål, A, (2021) Potential values of maas impacts in future scenarios. *Journal of Urban Mobility* 1. DOI: 10.1016/j.urbmob.2021.100005