vehicles

MDPI

Perspective

Perspectives on Securing the Transportation System

Raj Bridgelall

Transportation, Logistics & Finance, College of Business, North Dakota State University, P.O. Box 6050, Fargo, ND 58108-6050, USA; raj@bridgelall.com

Abstract: The vast, open, and interconnected characteristics of the transportation system make it a prime target for terrorists and hackers. However, there are no standard measures of transport system vulnerability to physical or cyberattacks. The separation of governance over different modes of transport increases the difficulty of coordination in developing and enforcing a common security index. This paper contributes a perspective and roadmap toward developing multimodal security indices that can leverage a variety of existing and emerging connected vehicle, sensing, and computing technologies. The proposed technologies include positive train control (PTC), vehicle-to-everything (V2X), weight-in-motion (WIM), advanced air mobility (AAM), remote sensing, and machine learning with cloud intelligence.

Keywords: cybersecurity; counterterrorism; vulnerability assessment; transportation security index

Citation: Bridgelall, R. Perspectives on Securing the Transportation System. *Vehicles* **2022**, *4*, 1332–1343. https://doi.org/10.3390/vehicles4040070

Academic Editors: Elżbieta Macioszek and Chen Lv

Received: 26 July 2022
Accepted: 22 November 2022
Published: 25 November 2022

1. Introduction

Growing population and commerce are placing increasing demands on the complex network of interacting modes and nodes that make up an open transportation system. Figure 1 illustrates many of those complex interactions among the various subsystems. The pressure to increase throughput grows steadily with increasing levels of international trade and gross domestic product (GDP) [1]. Emerging modes of transportation such as connected and autonomous vehicles (CAVs) that include cars, trucks, buses, pipelines, drones, and micromobility add cybersecurity challenges to the existing physical security risks. Meanwhile, resource constraints can result in complacency that create security gaps [2]. These characteristics make all modes of the transportation system attractive to perpetrators.

Previous attacks on the transportation network spotlighted vulnerabilities where small explosions created critical bottlenecks that catalyzed a rapid economic decline. For instance, the 2003 and 2009 plots to bomb the Brooklyn Bridge and the New York City Subway system, respectively, triggered a nationwide bomb alert that crippled mobility [3]. Terrorist organizations have demonstrated how the public transit system could be very efficient at spreading toxins such as chemical and biological weapons. One example is the sarin gas release into the Tokyo subway system in 1995 [4]. The series of 2017 bombings of passenger trains in Asia and Europe are more recent examples of the system's vulnerability to physical attacks. More recently, the 2021 ransomware attack on the U.S. Colonial Pipeline and its temporary shutdown triggered public panic that resulted in fuel hoarding [5].

To keep the transportation system open and efficient, it is not practical or cost-effective to protect every possible vulnerable portal with armed guards or technology. Transportation agencies must measure and report the international roughness index (IRI) of pavements in their jurisdiction to justify federal funding for maintenance. However, there are no equivalent security indices to assess risks for focused remediation. Hence, the main contributions of this work are perspectives on leveraging emerging technologies to feed the development and standardization of multimodal risk indices that mirrors the purpose of the IRI. The requirement to quantify and report a simple risk index will reduce complacency in securing the transportation system because humans tend to improve what gets measured [6]. Hence,

this paper contributes a research roadmap toward developing a set of risk indices that leverage existing and emerging connected vehicle, sensing, and computing technologies. The contribution includes defining a simple security index and demonstrating its utility via a simulated risk scenario. The idea of promoting the reporting of a standard security index is to elicit a gradual change in mindset towards transportation security from being reactive to becoming more proactive. This work highlights the disjointed treatment of security across transport agencies and suggests a more coordinated and collaborative effort to develop associated policies to produce standard security indices that will lead to cost reduction, efficiency enhancements, deterrence, and improved preparedness. A requirement to report security indices will promote a culture of continuous vigilance and vulnerability assessments across all existing and emerging transportation modes and encourage designers to integrate security as an essential element rather than as an afterthought. The deployed technologies will enhance situational awareness and create "a curtain of uncertainty" that can help to deter threats.

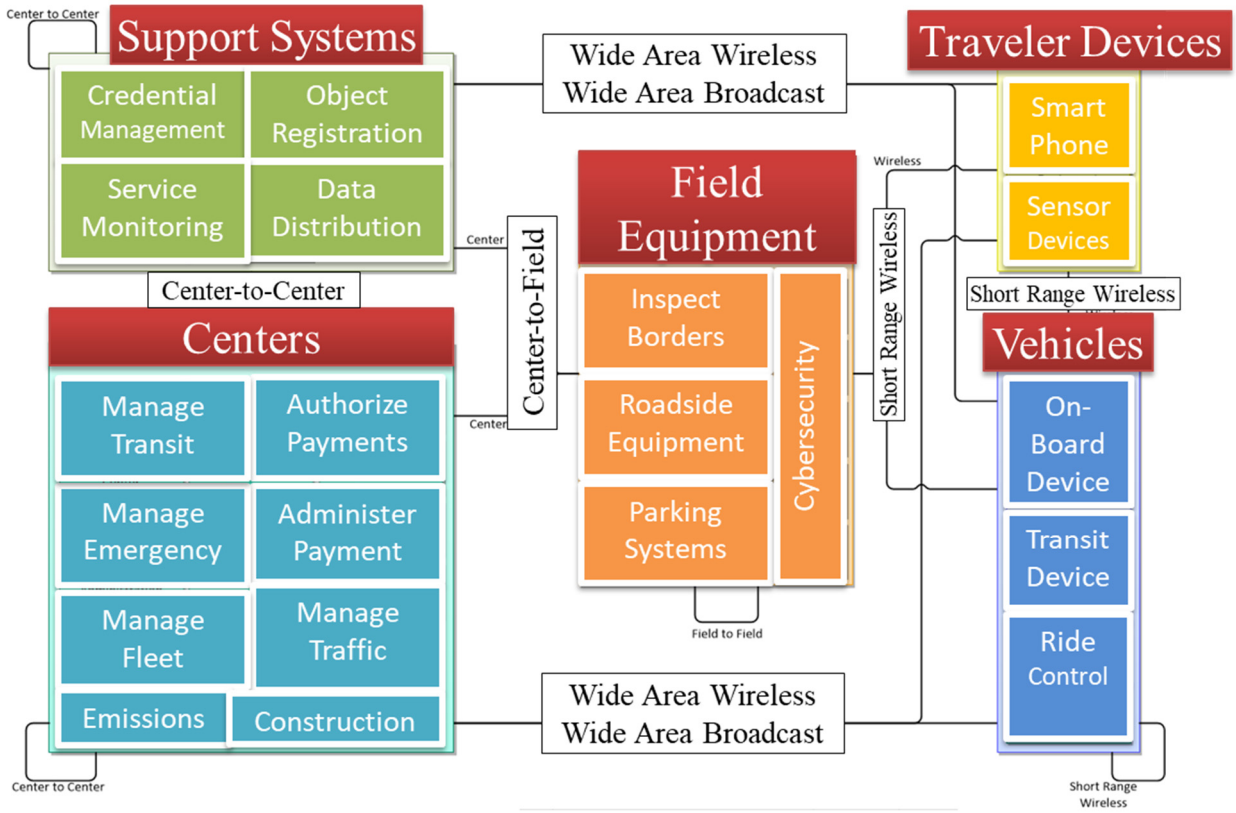

Figure 1. The connected transportation system.

The organization of the remainder of this paper is as follows: Section 2 presents the current situation of multimodal transportation system governance and security practices. Section 3 presents a perspective on modeling terrorist behavior as a complex adaptive system (CAS), proposes a three-stage research roadmap, discusses examples of simple security indices, and explores how existing technologies can inform the development of security indices. Section 4 concludes the proposal.

2. Current Situation

The primary challenges in implementing security are generally related to a lack of organizational cohesion and a lack of resources. Creating cohesive and coordinated transportation security policies across all modes will require close collaboration among the bureaucratic silos of federal, state, and local governments. Implementing security practices will also involve coordination and cooperation with private-sector organizations such as

competing freight carriers. Governments and private-sector organizations own and operate various modes of transportation within and across jurisdictional boundaries. Using the United States as a case study, various agencies of the federal government oversee the maintenance and safety of different transport modes. For example, state governments are generally responsible for maintaining all roads within their jurisdiction and receive matching funds from the Federal Highway Administration (FHWA) to maintain portions of the Interstate and the National Highway System (NHS) [7]. The Federal Motor Carrier Safety Administration (FMCSA) regulates the operation of commercial motor vehicles, but its primary mission is safety, not necessarily security [8]. Private sector organizations own and operate railroads and pipelines; however, they comply with safety regulations of the Federal Railroad Administration (FRA) and the Pipeline Hazardous Materials Safety Administration (PHMSA), respectively [9]. The Federal Transit Administration (FTA) provides financial and technical assistance to promote the safe and efficient operation of buses, passenger rail, and ferryboats of local and public transportation systems [10]. The Federal Aviation Administration (FAA) regulates and oversees all aspects of American civil aviation, including the integration of drones into the national airspace [11]. The United States Coast Guard (USCG) is a branch of the U.S. Department of Homeland Security (DHS), not the USDOT [12]. The USCG enforces U.S. maritime laws in both domestic and international waters. It is noteworthy that the missions of these organizations do not explicitly include transportation security. Rather, a separate organization, the Transportation Security Administration (TSA) is responsible for security across all transportation modes [13]. However, the TSA is an agency of the DHS, not the USDOT.

The U.S. Customs and Border Protection (CBP) is an agency of the DHS [14]. The primary mission of the CBP is to prevent terrorists and unauthorized weapons from entering the United States. The DHS absorbed the TSA from the USDOT two years after its formation. The overall DHS mission is to protect the United States and its territories from natural and fabricated threats [15]. The DHS provides grants to state and local governments to improve their ability to identify and protect against terrorist threats and attacks. Although the TSA collaborates with state, local, and regional partners to oversee security for highways, railroads, mass transit, pipelines, and ports, their effort has been historically more focused on aviation security [13]. Consequently, creating a coordinated and cohesive plan to promote security across all modes of transportation will be challenging. Even without congressional gridlock, such an undertaking in policy making will require many champions to forge a change in the mindset towards global transportation security.

3. Perspectives

The next four subsections provide a perspective on terrorist behavior, a research roadmap toward securing the transportation system, examples of simple risk indices found in the literature, and technologies that can help to create situational awareness.

3.1. Complex Adaptive Systems

Terrorist continually seek openings to exploit and adapt their strategies [16]. To stay one-step ahead, agencies must develop a mindset that the transportation system will never be completely secure and that they must continually assess and anticipate threats and adapt countermeasures. It is helpful to understand this concept of evolving threats and countermeasures as a complex adaptive system (CAS). Borrowing from a technical description of CAS by Holland (1992), terrorist groups have the following seven characteristics [17]:

AGGREGATION—like ant colonies, perpetrators have simpler sub-components that combine to form cohesive wholes and characteristic behaviors. This feature makes identification of any one terrorist agent exceedingly difficult because the group as an aggregate behaves like a larger organism.

TAGGING—identifying characteristics such as symbols that serve to create a brand that rally members of similar persuasion to join their cause. Fast image processing and

artificial intelligence techniques currently available can recognize symbols to help identify and track suspicious individuals or members of known terrorist originations.

NONLINEARITY—like insect colonies, individual parts do not equal the whole. Hence, it is difficult to eradicate threats completely by simply taking out one or more members, or even leaders.

FLOWS—a "resource" flows across a network where nodes, links, and flow rates change as the agents adapt. There is a multiplier effect as resources move along nodes. The agents recycle spent resources to accelerate growth. Hence, terrorists also rely on transportation networks to maintain mobility and accessibility of their resources.

DIVERSITY—in a Darwinian manner, the network produces many varieties that are essential for survival in changing environments. They have self-healing properties, and they adapt strategies and tactics.

INTERNAL MODEL—like bacteria swimming up the chemical (Glucose) gradient to increase chances of finding sustenance, agents use technology and sentinels to guide their strategy and tactics. Hence, terrorists will continually seek out modern technologies and tactics to identify and exploit security gaps.

BUILDING BLOCKS—to reduce energy use and cost, agents reuse components that have worked in the past. For example, terrorist groups recruit lonely and/or disturbed individuals because they tend to become loyal followers. Terrorists continue to attack transportation networks because doing so is efficient and brings attention to their agenda.

The above seven principles of CAS highlight the reason counterterrorism is not a one-time solution. Rather, counterterrorism and cybersecurity efforts must be continuous and adaptive. In essence, all transportation agencies must become security agents that proactively analyze the system for vulnerabilities and adapt countermeasures accordingly. They must also collaborate towards the same overall mission of achieving global transportation security.

3.2. Research Roadmap

The suggested near-term, mid-term, and long-term objectives of a research roadmap toward securing the transportation system are as follows:

Near-term: fund research efforts within 3 years to catalog, select, assess, and demonstrate the feasibility of existing and emerging technologies to enhance visibility of potential threats to the transportation system. Identify ideas and modern technology needs that will provide the greatest potential for treat deterrence and return on investment. Create research programs now by appropriating seed funds. Continue the funding cycle annually to focus research on transportation *security*, which is distinct from the focus on transportation *safety*.

Mid-term: coordinate relevant federal agencies, local jurisdictions, international partners, and the commercial sector to develop a standard *transportation risk index* (TRI) that can help with assessing and reporting risks to potential terrorist targets across all modes of transportation and their intermodal facilities. The standard should include guidelines for measuring and reporting the TRI within each mode. Standard risk indices can inform decisions to focus resources on the highest risk areas. Agencies can begin their request for information now and plan for ratification of relevant standards within 10 years.

Long-term: develop associated policies that would mandate the reporting of a TRI annually to qualify for *federal funding* from the respective modal transportation agencies. Develop a common web-based platform to educate and to accommodate standard TRI reporting procedures. Establish the resources that will analyze the TRI data to prioritize security enhancement projects. Begin to promote the idea now to create buy-in and spur policymaking. Plan to enact and enforce the policies within 15 to 20 years.

One perspective in developing a national security practice is that the Research and Innovative Technology Administration (RITA) of the USDOT will need to engage the DHS, TSA, NTSB, international partners, and various technology research and private sector organizations to coordinate complementary research efforts across transportation modes. In essence, the various government agencies would primarily play a strategic and adminis-

trative role to allocate and direct resources. States and local jurisdictions would assume the tactical role of investing in the appropriate deterrence planning, technology development, and end-user adoption. Another perspective in developing a national security practice is that RITA should also coordinate the national architecture, standardization, and guidelines development to facilitate the seamless integration of systems across jurisdictional boundaries. Local transportation agencies should guide technology manufactures to develop systems that are suitable for integration and operation within their jurisdictions.

3.3. Risk Indices

This section presents an example of a simple risk index and provides a scenario and case study to understand its application in focusing limited resources on the highest risk locations.

3.3.1. Design

One approach to define the TRI for a particular mode is to determine the probability of a terror incident at a particular node in the network. Next, multiply that probability by the population density within some standard distance of a centroid. The overall TRI for a location can be the simple summation of the TRIs for all centroids, across all modes operating within a jurisdictional boundary. Using a geographic information system (GIS) platform, agencies can visualize vulnerabilities spatially by color-coded TRI magnitudes and make informed decisions to prioritize funding accordingly. To normalize the reporting, the multimodal TRI for a location can be the average value across all nodes and modes.

3.3.2. Scenario Simulation

A town with a population density of 100 people per square mile has two routes through it, Route 1 and Route 2. The town installs a roadside sensor along Route 1 to detect passing vehicles that transport hazardous (radioactive) waste from a nearby hospital facility. Upon identifying the vehicle, the system interrogates the motor carrier database to verify the truck identification, payload type, expected gross weight, and planned route. If the Route 1 sensor operates with a missed detection probability of 10%, then the TRI for Route 1 will be:

$$TRI_{\text{roads}} = 100 \text{ persons/square-mile} \times 0.10 = 10. \quad (1)$$

In this scenario, there are no roadside sensors on Route 2. Therefore, the missed detection probability will be 100%, and the TRI for Route 2 will be $100 \times 1.00 = 100$. Hence, the total roadway TRI for the town consisting of only two routes is $TRI_{\text{roads}} = TRI_{\text{route1}} + TRI_{\text{route2}} = 10 + 100 = 110$.

In the above scenario, a carrier reported that one of its trucks carrying radioactive waste along Route 1 was missing. It turned out that hijackers stole the truck and exited the town along Route 2. After days of searching, the authorities found the vehicle and its payload abandoned on a nearby farm. In reaction, the town promptly installed a roadside detector along Route 2. However, this detector was less expensive and has a missed detection probability of 20% (versus 10%). Nevertheless, the Route 2 TRI dropped from 100 to $(100 \times 0.20) = 20$. Hence, the total road TRI for the town dropped from 110 to 30.

To qualify for federal assistance, the town must also compute the TRI for pipelines, railroad segments, and other modal facilities within its authority. It is likely that a policy to regularly assess and report the TRI of a location would lead to continuous awareness and possibly a change in mindset as investments, grants, and innovations force a lower risk index over time. The town, in essence, will achieve what it is measuring—a lower TRI. Bridgelall (2022) provided other examples of how to derive a risk index for public transit by using artificial intelligence [18], and for maritime facilities by using the RAMCAP model [19].

3.3.3. Real Case Study

In December 2013, hijackers in Mexico stole a truck transporting Cobalt-60, a highly radioactive material. Hijackers repeated this incident in July 2014 when they stole a truck containing Iridium 192. Each time, Mexican authorities found the truck abandoned with its radioactive payload discarded some distance away. Had this been a terrorist activity, the delay in finding the vehicle could have led to a disaster. That is, the hijackers could have released the harmful materials in a large city along the way.

Radiation sensors anywhere along the truck route would have detected the radioactive material. However, the warning decals on the stolen truck were still intact; therefore, lower cost technologies, such as optical image recognition, would have detected the truck, and real-time database lookup of the carrier route plan would have revealed that the truck had been diverted. Had such a sensor node existed along the route, the truck would not have escaped after the system alerted enforcement agents.

3.4. Surveillance Technologies

The National Transportation Safety Board (NTSB) investigates accidents, crashes, and hazardous material releases that involve railways, pipelines, airways, marine, and some types of highway incidents. The NTSB maintains and promotes a "Most Wanted List" of transportation safety improvements [20]. Practitioners often credit the NTSB with inspiring a variety of multimodal technologies and policies to improve safety. These include mid-air collision sensors, age-21 drinking laws, smart airbag deployment, commercial driver's licenses, railroad anti-collision systems, fire drills on cruise ships, pipeline corrosion coatings, and drug/alcohol testing.

RITA is responsible for the advancement of transportation science, technology, and analysis. Hence, RITA will likely be the most suitable agency to spearhead an effort to identify, assess, and demonstrate the performance of technologies suitable for enhancing transportation security and informing a security index. RITA could collaborate with the NTSB to coordinate and fund such research. Figure 2 illustrates the author's perspective on how to automate the generation and reporting of transport security indices.

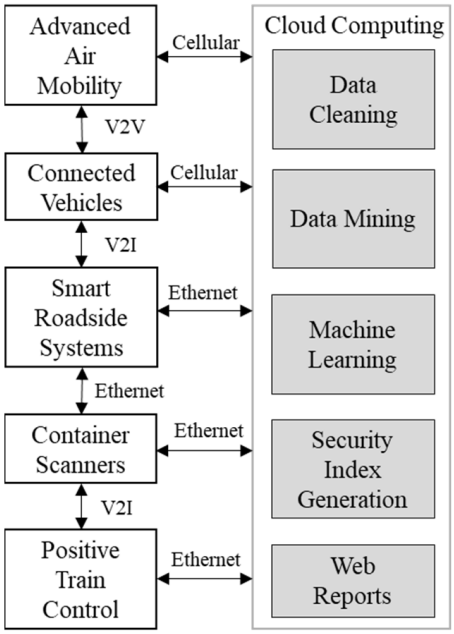

Figure 2. The integration of emerging technologies to generate and report transport security indices.

The next sections highlight some of the existing technologies that can be used to extend tools in transportation security surveillance.

3.4.1. Connected Vehicles

The USDOT has been leading a long-term coordination with road vehicle manufacturers and the private sector to demonstrate the feasibility and utility of connected vehicle technologies [21]. The USDOT envisions a future where all types of roadway vehicles "talk" with each other to avoid collision and maintain an Internet connection to exchange information that would enhance travel safety and infrastructure capacity. The program also attempted to address the privacy concerns of travelers and shippers [22]. Citizens continuously raise concerns about the legality of connected vehicle systems with respect to their civil liberties [23]. Such systems are also vulnerable to cyberattacks because of the many entry points for malicious software [24].

Despite their vulnerabilities, this work suggests that connected vehicles can be used in unconventional ways to enhance security. For instance, cloud systems that track passenger actions in shared rides can trigger alerts upon the detection of behavioral anomalies. Connected cloud systems can also track the behavior of freight vehicles continuously, and scan for vulnerabilities in the roadway infrastructure based on uploaded sensor data. Communications with intelligent traffic lights can detect anomalies in signal timing to identify system control tampering. Sharing the communications history with other vehicles and uploading the data to cloud systems can enable artificial intelligence methods to detect changes in normal communications. Similarly, any communications with pedestrian devices that appear to be anomalous can trigger further investigation.

3.4.2. Smart Roadside Systems

The connected vehicle program spawned the smart roadside initiative (SRI) to demonstrate existing technologies that can conduct safety inspections of commercial motor vehicles at mainline speeds [21]. Figure 3 is the author's rendition of a basic smart roadside inspection system that communicates information about a freight vehicle by using the SAE J1939 and vehicle-to-infrastructure (V2I) communications standards.

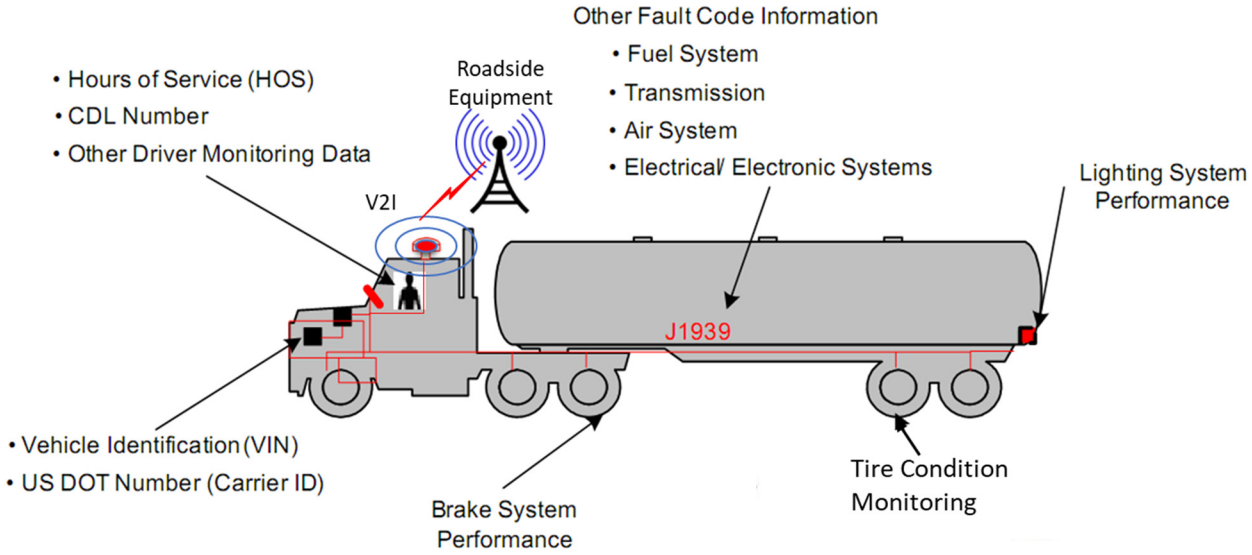

Figure 3. Concept of a Smart Roadside System.

Other systems such as automatic license plate readers (ALPRs), RFID tags, and/or electronic onboard recorders or smartphone apps communicate with roadside equipment or Internet systems to identify vehicles, their carrier, and the driver in some cases [25]. Road embedded weigh-in-motion (WIM) scales determine the weight of vehicles, and light detecting and ranging (LiDAR) systems measure vehicle dimensions while in motion [26]. A software system automatically determines the "oversize/overweight" and "credential" status of the vehicle and its operator to select for further manual scrutiny those with a high

potential for non-compliances. Some implementations also integrate high-speed radioactive detectors and infrared imagers at the roadside to detect unauthorized hazardous cargo movements [27]. Even though the technologies exist, and broad enforcement policies can reduce risks for everyone, carriers criticize aspects of these types of systems for privacy and business confidentiality violations [21]. Consequently, agencies have postponed the deployment of such automatic identification and safety monitoring systems.

3.4.3. Container Scanners

The intermodal container is arguably the most important innovation in freight transportation. It improves handling efficiency and damage susceptibility by transporting a standard dimension and locked unit across ship, rail, and truck modes. Most of these containers are part of international trade routes and hence pose a significant security threat. The DHS implemented a goal of 100% cargo scanning by 2012 and invested in the development of gamma-ray and X-ray radiography [28]. Such devices direct a beam of atomic particles through the steel containers [29]. Detectors on the other side of the emitter capture images to identify regions of high density that are possibly signatures of human stowaways or nuclear material. Although effective, such systems are expensive and slow. They result in significant reductions of port throughput [19].

The TSA introduced a similar backscatter X-ray imaging technology in 2010 to detect any hidden explosives on or within the bodies of passengers. If the system detects an anomaly, the person gets a "pat-down" which has raised significant public outcry about privacy and health concerns [2]. These electromagnetic scanners resulted in numerous lawsuits to halt the practice on the grounds of fourth amendment (unreasonable searches and seizures) violations [2]. Nevertheless, with sufficient market demand, companies will likely improve the technology and reduce their costs.

3.4.4. Positive Train Control

Figure 4 is the author's rendition of a positive train control (PTC) system.

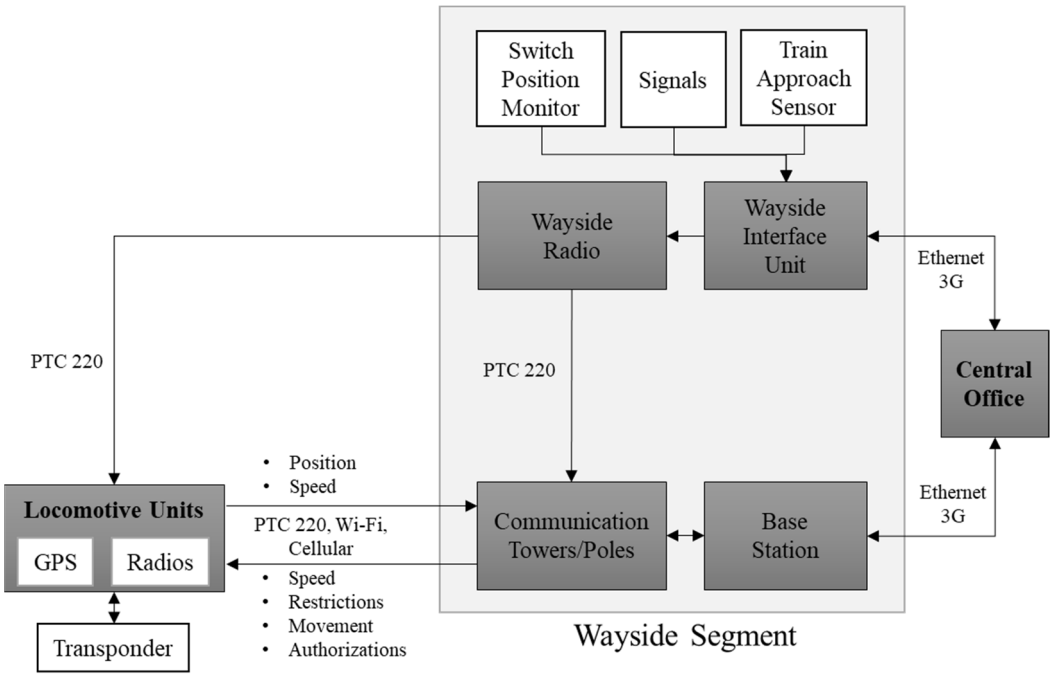

Figure 4. Architecture of a PTC system.

Positive train control (PTC) is a centralized control system prevent accidents by monitoring and orchestrating train movements [30]. The U.S. Congress mandated full implementation of PTC by the end of 2020. PTC uses a myriad of technologies to enforce speed limits,

train separation distances, and wayside worker safety. PTC implementations combine RFID, global positioning system (GPS) receivers, and inertial navigation systems (INS) to identify the position of a train, including during satellite outages [31]. The contributed perspective is that agencies using PTC can leverage the data to inform the development of a railroad security index that accounts for traffic density, freight type, and population densities nearby.

3.4.5. Next Gen and Advanced Air Mobility

The FAA has been promoting the use of GPS and automated vehicle navigation technologies to transform the existing control system for air traffic from a ground-based to a satellite-based system [32]. The higher position accuracy of GPS will allow for closer aircraft spacing, leading to substantial increases in system capacity. In a related program called advanced air mobility (AAM), the FAA is coordinating with industry to support the integration of passenger and cargo drones into the national airspace [33]. Other than the typical concerns about cost and reliability, the main criticism of this position-tracking technology has been its delay in the FAA approval process and the subsequent policy making. No technology is fail-safe. These types of vehicle navigation and guidance systems depend heavily on the reliability of satellites to provide both communications and geospatial positioning data, all of which can fail for numerous reasons at any time. For example, strong solar flares can be a source of significant electromagnetic disruptions for such airborne systems [34].

AAM technology is rapidly evolving towards commercial launch between 2025 and 2030 [35]. However, there are still many barriers to adoption, including a lack of regulations and standards [36]. Early adopters will use drones for medical cargo transport to hospitals and remote facilities [37], delivery of pharmaceuticals to homes and communities [38], and for humanitarian missions and disaster relief [39]. The early majority will deploy cargo drones for last-mile package delivery [40]. The rapid and sustained growth of e-commerce has led to a growing demand for same day and even same hour deliveries [41]. Consequently, logistics providers are experimenting with hybrid truck-drone systems to deliver packages in neighborhoods [42]. The contributed perspective is that all drone service providers can offer their data, including images captured and sensor feeds, to cloud-based security analysts that update and maintain transport security indices.

3.4.6. Remote Sensing and GIS

Transport agencies are now using drones to estimate traffic density [43] and to monitor the condition or railroads, bridges, and roads [44]. The emergence of stereo and high-resolution satellite imaging, and the evolving capabilities of low-cost commercial drones to transmit high-resolution multispectral and hyperspectral images from low altitudes hold enormous promise in vulnerability assessment [45]. Hyperspectral cameras can "see" beyond the spectral range of human vision. Such systems can detect hidden or covered objects on the ground, for example, vehicles and weapons hidden under foliage. Pipeline and railroad operators can use hyperspectral imaging to identify right-of-way encroachments and other vulnerabilities. Urban planners routinely couple remote sensing with GIS to analyze the transportation network for capacity bottlenecks and potential safety issues [44]. The contributed perspective is that agencies can use remote sensing to characterize the vulnerability of bridges, rail grade crossings, and hazardous material transloading facilities. Some of the current downsides of remote sensing systems are the cost and latency of the data gathering and analysis. As with other types of surveillance technologies, remote sensing provokes concerns about privacy.

3.4.7. Machine Learning and Data Mining

Algorithms to identify patterns in exceptionally large datasets (big data) are continuously emerging. The concept of teaching machines to learn from data and adapt rather than follow some predetermined set of logic has existed for decades. However, the steady

pace of increasing processor capabilities, hardware cost reduction, and competition to offer cloud-services are now making these technologies affordable. Data mining methods include statistical analysis of databases to classify events, and the application of neural networks to learn patterns that are otherwise difficult to characterize by theoretical modeling [46]. Transportation agencies can use such tools to train computers to identify suspicious behaviors and movements involving hazardous materials [47]. The TSA implemented a behavioral analysis system to identify suspicious passengers [14], but the practice led to concerns of racial profiling. Facial and symbol (decal) recognition algorithms are continuously evolving to deliver greater accuracy in mixed and noisy scenes. However, false positives could lead to significant public backlash. The contributed perspective is that data mining, machine learning, and artificial intelligence in the cloud can help inform the development, maintenance, and standardization of transport security indices across all modes of transportation.

4. Conclusions

Modeling the behavior of terrorists as complex adaptive systems (CAS) teaches us that perpetrators will continue to seek out and exploit vulnerabilities in the transportation system. Consequently, a mostly reactive approach to transportation security will continue to leave vulnerability gaps that can result in costly and catastrophic events. To be effective, proactive approaches such as regular vulnerability and risk assessments must be cohesive and integrate all modes. Agencies worldwide could capitalize on the rapid cost and size reduction of a myriad of existing and emerging technologies such as connected vehicles and machine learning to augment global transportation security. However, technology itself is not a panacea. Governments worldwide must implement policies that enhance coordination amongst governing agencies and promote a change in mindset towards security. Regular measures of *performance* currently encourage long-term planning to improve the condition of the transportation system. Similarly, an extension of those measures to include regular risk assessments by reporting a standardized risk index will likely yield a similar focus towards keeping the transportation system secure.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. USDOT. *Supply Chain Assessment of the Transportation Industrial Base: Freight and Logistics*; United States Department of Transportation (USDOT): Washington, DC, USA, 2022. Available online: https://www.transportation.gov/supplychains (accessed on 20 July 2022).
2. CRS. *Transportation Security: Background and Issues for the 117th Congress*; Congressional Research Service (CRS): Washington, DC, USA, 2021. Available online: https://crsreports.congress.gov/product/pdf/R/R46678 (accessed on 20 July 2022).
3. Krueger, A. What makes a homegrown terrorist? Human capital and participation in domestic Islamic terrorist groups in the USA. *Econ. Lett.* **2008**, *101*, 293–296. [CrossRef]
4. Beaton, R.; Stergachis, A.; Oberle, M.; Bridges, E.; Nemuth, M.; Thomas, T. The sarin gas attacks on the tokyo subway 10 years later/lessons learned. *Traumatology* **2005**, *11*, 103–119. [CrossRef]
5. Corbet, S.; Goodell, J.W. The reputational contagion effects of ransomware attacks. *Financ. Res. Lett.* **2022**, *47*, 102715. [CrossRef]
6. Drucker, P.F. *The Effective Executive: The Definitive Guide to Getting the Right Things Done*; Harper Business: New York, NY, USA, 2006.
7. FHWA. *Demonstrating the Application of Life Cycle Planning (LCP) on a Pavement Network*; Federal Highway Administration (FHWA): Washington, DC, USA, 2022. Available online: https://www.fhwa.dot.gov/asset/pubs/hif21044.pdf (accessed on 20 July 2022).
8. FMCSA. *2021 Pocket Guide to Large Truck and Bus Statistics*; Federal Motor Carrier Safety Administration (FMCSA): Washington, DC, USA, 2022. Available online: https://www.fmcsa.dot.gov/safety/data-and-statistics/2021-pocket-guide-large-truck-and-bus-statistics (accessed on 20 July 2022).
9. PHMSA. *2020 Emergency Response Guidebook*; Department of Transportation, Pipeline and Hazardous Materials Safety Administration (PHMSA): Washington, DC, USA, 2020. Available online: https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2020-08/ERG2020-WEB.pdf (accessed on 20 July 2022).

10. FTA. *Sample Safety Risk Assessment Matrices for Bus Transit Agencies*; Federal Transit Administration (FTA): Washington, DC, USA, 2019.
11. FAA. *Urban Air Mobility: Concept of Operations, v1.0.*; Federal Aviation Administration (FAA): Washington, DC, USA, 2020. Available online: https://nari.arc.nasa.gov/sites/default/files/attachments/UAM_ConOps_v1.0.pdf (accessed on 20 July 2022).
12. GAO. *Coast Guard: Information on Defense Readiness Mission Deployments, Expenses, and Funding*; Government Accountability Office (GAO): Washington, DC, USA, 2021. Available online: https://www.gao.gov/products/gao-21-104741 (accessed on 20 July 2022).
13. GAO. *Aviation Security Technology: TSA Lacks Outcome-Oriented Performance Measures and Data to Help Reach Objectives to Diversify its Marketplace*; Government Accountability Office (GAO): Washington, DC, USA, 2021. Available online: https://www.gao.gov/products/gao-21-146 (accessed on 20 July 2022).
14. GAO. *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections*; Government Accountability Office (GAO): Washington, DC, USA, 2022. Available online: https://www.gao.gov/products/gao-22-106100 (accessed on 20 July 2022).
15. GAO. *Border Patrol: Actions Needed to Improve Checkpoint Oversight and Data*; Government Accountability Office (GAO): Washington, DC, USA, 2022. Available online: https://www.gao.gov/products/gao-22-104568 (accessed on 20 July 2022).
16. Bridgelall, R. An Application of Natural Language Processing to Classify What Terrorists Say They Want. *Soc. Sci.* **2020**, *11*, 23. [CrossRef]
17. Holland, J.H. Complex Adaptive Systems. *Daedalus* **1992**, *121*, 17–30. Available online: http://www.jstor.org/stable/20025416 (accessed on 20 July 2022).
18. Bridgelall, R. Using artificial intelligence to derive a public transit risk index. *J. Public Transp.* **2022**, *24*, 100009. [CrossRef]
19. Patterson, D.A.; Bridgelall, R. Attack risk modelling for the San Diego maritime facilities. *Mar. Policy* **2020**, *121*, 104210. [CrossRef]
20. NTSB. *2021–2022 NTSB Most Wanted List of Transportation Safety Improvements. National Transportation Safety Board (NTSB)*. Available online: https://www.ntsb.gov/Advocacy/mwl/Pages/default.aspx (accessed on 17 July 2022).
21. USDOT. *Connected Vehicles*; United States Department of Transportation (USDOT): Washington, DC, USA, 2022. Available online: https://www.its.dot.gov/cv_basics/index.htm (accessed on 17 July 2022).
22. Yoshizawa, T.; Singelée, D.; Muehlberg, J.T.; Delbruel, S.; Taherkordi, A.; Hughes, D.; Preneel, B. A Survey of Security and Privacy Issues in V2X Communication Systems. *ACM Comput. Surv. CSUR* **2022**. [CrossRef]
23. Acharya, S.; Mekker, M. Public acceptance of connected vehicles: An extension of the technology acceptance model. *Transp. Res. Part F Traffic Psychol. Behav.* **2022**, *88*, 54–68. [CrossRef]
24. Salek, M.S.; Khan, S.M.; Rahman, M.; Deng, H.-W.; Islam, M.; Khan, Z.; Shue, M. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *IEEE Internet Things J.* **2022**, *9*, 8250–8268. [CrossRef]
25. USDOT. *Smart Roadside Initiative: Concept of Operations*; United States Department of Transportation (USDOT): Washington, DC, USA, 2015. Available online: https://rosap.ntl.bts.gov/view/dot/3562 (accessed on 20 July 2022).
26. Zhang, Z.; Huang, Y.; Bridgelall, R.; Palek, L.; Strommen, R. Sampling optimization for high-speed weigh-in-motion measurements using in-pavement strain-based sensors. *Meas. Sci. Technol.* **2015**, *26*, 065003. [CrossRef]
27. USDOT. *Smart Roadside Initiative Gap Analysis: Trucking Technology Literature Review*; United States Department of Transportation (USDOT)): Washington, DC, USA, 2014. Available online: https://rosap.ntl.bts.gov/view/dot/3532 (accessed on 20 July 2022).
28. GAO. *Air Cargo Security: TSA Field Testing Should Ensure Screening Systems Meet Detection Standards*; United States Government Accountability Office (GAO): Washington, DC, USA, 2021. Available online: https://www.gao.gov/assets/gao-21-105192.pdf (accessed on 20 July 2022).
29. Orphan, V.J.; Muenchau, E.; Gormley, J.; Richardson, R. Advanced γ ray technology for scanning cargo containers. *Appl. Radiat. Isot.* **2005**, *63*, 723–732. [CrossRef] [PubMed]
30. Hooey, B.L.; Marfise, E.; Broderickl, P.; Weaver, L.; Pina, B. *Positive Train Control (PTC) Study: An Analysis of PTC-Related Reports Submitted to the Confidential Close Call Reporting System (C3RS). Moffett Field, California: National Air and Space Administration (NASA)*; 2021. Available online: https://www.sti.nasa.gov/ (accessed on 20 July 2022).
31. Kolli, S.; Lilly, J.; Wijesekera, D. Positive train control security: An intrusion-detection system to provide cyber-situational awareness. *IEEE Veh. Technol. Mag.* **2018**, *13*, 48–60. [CrossRef]
32. GAO. *Transforming Aviation: Stakeholders Identified Issues to Address for 'Advanced Air Mobility'*; Government Accountability Office (GAO): Washington, DC, USA, 2022. Available online: https://www.gao.gov/products/gao-22-105020 (accessed on 20 July 2022).
33. Lineberger, R.; Silver, D.; Hussain, A. *Advanced Air Mobility: Can the United States Afford to Lose the Race? Deloitte Development LLC*. 2021. Available online: https://www2.deloitte.com/us/en/insights/industry/aerospace-defense/advanced-air-mobility.html (accessed on 20 July 2022).
34. Dempster, A.G. GNSS Vulnerability: A Taxonomy. In *Positioning and Navigation in Complex Environments*; Dempster, A.G., Ed.; IGI Global: Hershey, PA, USA, 2018; pp. 515–531. [CrossRef]
35. Merkert, R.; Bushell, J. Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control. *J. Air Transp. Manag.* **2020**, *89*, 101929. [CrossRef] [PubMed]
36. Sah, B.; Gupta, R.; Bani-Hani, D. Analysis of barriers to implement drone logistics. *Int. J. Logist. Res. Appl.* **2021**, *24*, 531–550. [CrossRef]

37. Grote, M.; Cherrett, T.; Oakey, A.; Royall, P.G.; Whalley, S.; Dickinson, J. How do dangerous goods regulations apply to uncrewed aerial vehicles transporting medical cargos? *Drones* **2021**, *5*, 38. [CrossRef]
38. Royall, P.G.; Courtney, P. Medicine delivery by drone–Implications for safety and quality. *Eur. Pharm. Rev.* **2019**, *24*, 48–51.
39. Rabta, B.; Wankmüller, C.; Reiner, G. A drone fleet model for last-mile distribution in disaster relief operations. *Int. J. Disaster Risk Reduct.* **2018**, *28*, 107–112. [CrossRef]
40. Kim, J.; Moon, H.; Jung, H. Drone-based parcel delivery using the rooftops of city buildings: Model and solution. *Appl. Sci.* **2020**, *10*, 4362. [CrossRef]
41. Kim, S.H. Choice model based analysis of consumer preference for drone delivery service. *J. Air Transp. Manag.* **2020**, *84*, 101785. [CrossRef]
42. Chung, S.H.; Sah, B.; Lee, J. Optimization for drone and drone-truck combined operations: A review of the state of the art and future directions. *Comput. Oper. Res.* **2020**, *123*, 105004. [CrossRef]
43. Doole, M.; Ellerbroek, J.; Hoekstra, J. Estimation of traffic density from drone-based delivery in very low level urban airspace. *J. Air Transp. Manag.* **2020**, *88*, 101862. [CrossRef]
44. Gupta, A.; Afrin, T.; Scully, E.; Yodo, N. Advances of UAVs toward future transportation: The State-of-the-Art, challenges, and Opportunities. *Future Transp.* **2021**, *1*, 326–350. [CrossRef]
45. Bridgelall, R.; Rafert, J.B.; Tolliver, D.D. Performance of hyperspectral imaging with drone swarms. *Transp. Res. Rec.* **2018**, *2672*, 36–44. [CrossRef]
46. Aggarwal, C.C. *Data Mining*; Springer International Publishing: New York, NY, USA, 2015.
47. Wei, S.; Shen, X.; Shao, M.; Sun, L. Applying Data Mining Approaches for Analyzing Hazardous Materials Transportation Accidents on Different Types of Roads. *Sustainability* **2021**, *13*, 12773. [CrossRef]