Journal of Transportation Security (2021) 14:137–155
https://doi.org/10.1007/s12198-021-00230-w

Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies

Bo Zou[1] · Pooria Choobchian[1] · Julie Rozenberg[2]

Received: 2 July 2020 / Accepted: 10 February 2021 / Published online: 8 March 2021

Abstract

The increasing cyber connectivity of vehicles and between vehicles and infrastructure will drastically reshape mobility in the coming decades. While the advent of connected mobility is expected to benefit travelers and the society by smoothing traffic, improving rider convenience, and reducing accidents, the augmented cyber components in connected and autonomous vehicles and related infrastructure also give rise to cyber-attacks to the transportation system. And yet, little attention has been paid to transportation cyber resilience. This paper thus proposes an investigation on this topic with a comprehensive literature review. The cyber components and plausible autonomous mobility systems (AMS) operation scenarios are discussed, before identifying possible cyber-attacks to AMS at both vehicle and system levels. The discussion then moves to existing practices to enhance cybersecurity, and a number of strategies are investigated toward enhancing AMS cyber resilience. At the vehicle level, creating layers and separation to reduce cyber component connectivity and deploying an independent procedure for data collection and processing are important in vehicle design and manufacturing. At the system level, recommended strategies include keeping redundancy in transportation capacity, maintaining a separate road network, and deploying different sub-autonomous mobility systems.

Keywords Autonomous mobility systems · Cyber resilience · Cyber-attacks · Vehicle- and system-level strategies

JEL classification R42 R48

✉ Bo Zou
bzou@uic.edu

[1] University of Illinois at Chicago, Chicago, IL, USA

[2] World Bank Group, Washington, D.C., USA

Introduction

The objective of this paper is to understand cyber resilience of transportation systems with a focus on future autonomous mobility. Cyber resilience is becoming a prominent issue in transportation as an increasing number of vehicles are Internet—and more generally cyber—connected. Taking the US as an example, currently about 50 million vehicles or 20% of all vehicles on the road have Internet connectivity. All major car manufacturers have been committed to adding more connectivity features to their upcoming models. As a result, it is estimated that about 17 million new "connected cars" will be added to the US roads each year (Consumer Watchdog 2019). These vehicles will be interconnected through not only cyber components in the vehicles, but also the associated infrastructure.

While the increased cyber connectivity is expected to enhance vehicle control, communication, and diagnostic functions which contribute to improved vehicle- and system-level functioning and mobility management, cyber connectivity also exposes vehicles and the mobility system to significant risks of cyber-attacks. Yet, little is known about what can be done to prepare the increasingly cyber connected vehicles and the mobility system for potential cyber-attacks. Anticipating the growing trend of vehicle cyber connectivity and the eventual dominance of autonomous vehicles—which will be even more cyber connected—in the future mobility environment, this paper takes a forward-looking view by focusing on ways to enhance the cyber resilience of autonomous mobility systems (AMS). Various types of cyber-attacks on AMS will be investigated and strategies to enhance AMS cyber resilience will be explored. Given the interdisciplinary nature of transportation cyber resilience, our investigation and exploration are based on a comprehensive, multifaceted literature review through journal articles and technical reports from disciplines including transportation engineering, computer science, electrical engineering, systems engineering, urban planning, and public policy. The review and subsequent analysis provide the building blocks for understanding the current practices and prospective strategies for AMS cyber resilience enhancement.

It is worth highlighting that although the focus of the paper is on AMS, many of the findings can inform enhancing cyber resilience of today's transportation systems given the common feature of cyber connectivity. In fact, as AMS is yet to be deployed, many discussions in the paper draw insights from research and experimentation on today's connected vehicles and transportation systems. In the ensuing section, we first discuss the cyber components in AMS and plausible AMS operation scenarios. Understanding the AMS operation scenarios is a premise besides understanding cyber-attacks to design effective measures to enhance AMS cyber resilience. A variety of plausible types of cyber-attacks, at both vehicle and system levels, are explored in the context of AMS in Section 3. In view of the AMS cyber components, operations scenarios, and cyber-attack types, Section 4 is dedicated to the concept of cyber resilience in the context of AMS, and practices and possible strategies to enhance AMS resilience. A summary is given in Section 5.

Future autonomous mobility systems

Cyber components in an autonomous vehicle

In autonomous mobility systems, self-driving vehicles are smart enough to constantly make routing and navigating decisions in a physical road network given existing/predicted vehicular traffic streams. The routing and navigating capability of AVs depends critically on the cyber components and their interactions with the physical parts of AVs and associated infrastructure. Indeed, it is the cyber components and the cyber-physical interactions, much more complex than in today's vehicles and transportation systems, that distinguish AMS from today's transportation systems.

The cyber components and functions are embedded in the sensors and network connectivities of AVs. Figure 1 illustrates the different sensing technologies that will be essential for information collection and the sense-and-avoidance capability of an AV. Dedicated short-range communication further enables vehicle-to-vehicle and vehicle-to-infrastructure communications for sending and receiving critical data such as road condition, congestion, crashes, and possible rerouting. Dedicated short-range communication also enables platooning, i.e., a train of AVs that travel together collectively. The information collected will be processed through a central onboard computing unit that outputs routing and navigating decisions. However, all these cyber components and functions are subject to cyber-attacks.

Plausible AMS operation scenarios

Since AVs in an AMS do not rely on human drivers, the way future mobility would look quite differently from what it is today. While research on future transportation with AVs has been booming, a consensus has not been achieved on the exact operation

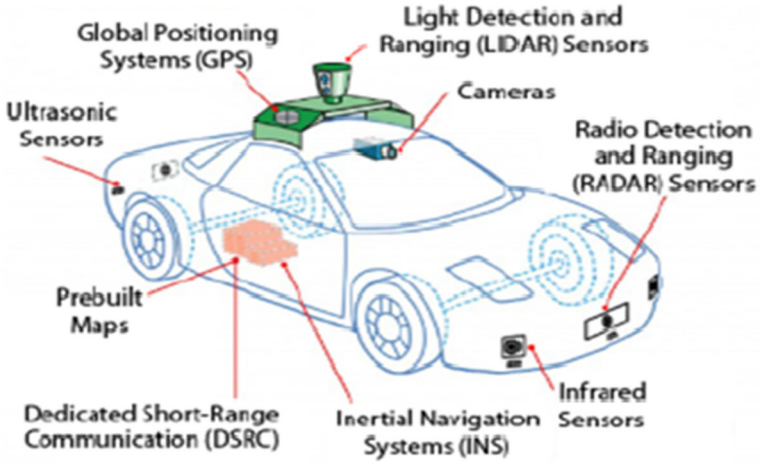

Fig. 1 Sensors and other technologies in a future AV (source: Center for Sustainable Systems 2018)

scenario of future transportation systems. Three plausible scenarios have attracted most attentions:

- *Autonomous mobility with private ownership:* In this scenario, most vehicles running on the street will be driverless and owned by individual households (Noruzoliaee et al. 2018). In addition, the possibility of household members coordinating schedules so that a single AV can accommodate their daily activities has been investigated (Cokyasar and Larson 2020). Relevant research has been further extended to looking into AVs co-ownership by residents in a neighborhood or a community (Masoud and Jayakrishnan 2017), which can reduce ownership cost of each individual and increase use flexibility.
- *Shared autonomous mobility:* The second scenario also conceives a world dominated by AVs. However, these AVs will be assets of large fleet operators such as a driverless version of future transportation network companies such as Uber and Lyft. Given that all major auto manufacturers nowadays are partnering with AV technology companies and/or developing AVs independently, it is possible that auto manufacturers may also become AV mobility service providers.
- *A mixed private and shared autonomous mobility with coexistence of human-driven vehicles:* This may be the most plausible scenario considering the long transition time from today to a complete self-driving environment, which may take at least a few decades (Fig. 2). A mixed traffic will persist on the road including privately owned human-driven vehicles, shared human-driven vehicles, privately owned AVs, and shared AVs (see Fig. 3 which forecast the total miles driven in the United States). The coexistence of the four types of vehicles would make traffic control very complex and challenging for modeling and analysis (Noruzoliaee and Zou 2021).

Note that most transportation systems of today have car and non-car modes. The coexistence of different modes is also expected to persist in the foreseeable future. Public transportation is an important non-car mode in helping mitigate traffic congestion, energy use, and emissions. In a future AMS, alternative modes other than AVs,

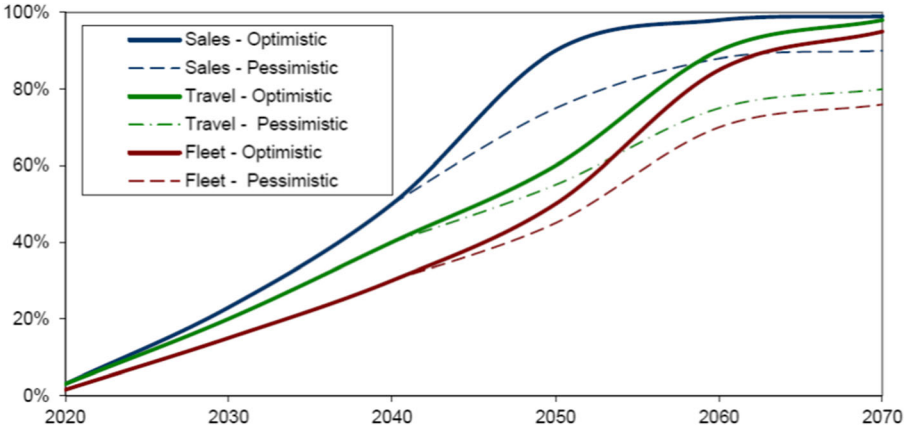

Fig. 2 AV sales, travel, and fleet projections (source: Litman 2018)

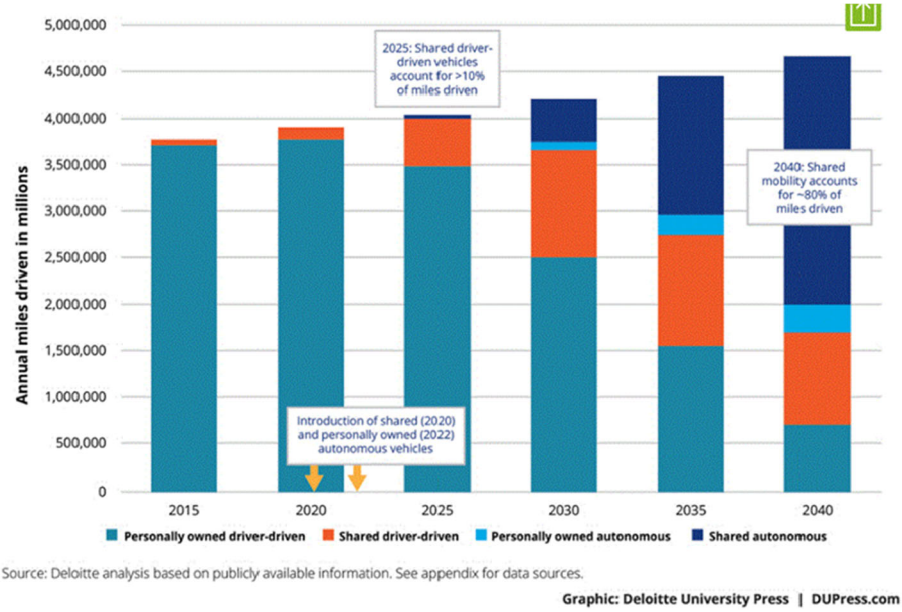

Fig. 3 Projection of annual vehicle miles traveled by different vehicle types: 2015–2040 (source: Deloitte 2016).

especially those that could be immune to cyber-attacks, would be necessary to offer transportation capacity when the AMS is affected by cyber-attacks. Joint considerations of AMS and alternative modes will therefore have important implications for enhancing AMS cyber resilience. This will be discussed in Section 4.

Cyber-attacks in the context of AMS

A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization (Cisco 2019). In the context of AMS, the breaching of the information system of AMS, which includes individual cyber devices, infrastructure, and networks for sensing, computing, and communication, is usually aimed at compromising key functions of the system for the benefits of the attackers. Cyber-attacks will cause harmful consequences to jeopardize the operational efficiency, safety, and privacy of AMS.

The breaching the AMS information system is realized by cyber-attackers successfully exploiting cyber vulnerabilities of AMS, which exist at both individual vehicle and system levels. At the vehicle level, cyber vulnerabilities arise due to a significant number of interfaces and communication networks in AVs as compared to conventional vehicles, which allow for greater exposure of AVs to external environment. At the system level, cyber vulnerabilities can result from: 1) inadequate schemes for data access control between AMS and the external environment as well as within AMS; 2) lack of coordination among cyber component providers and AV manufacturers; and 3) AMS developers and mobility service providers not paying enough attention to

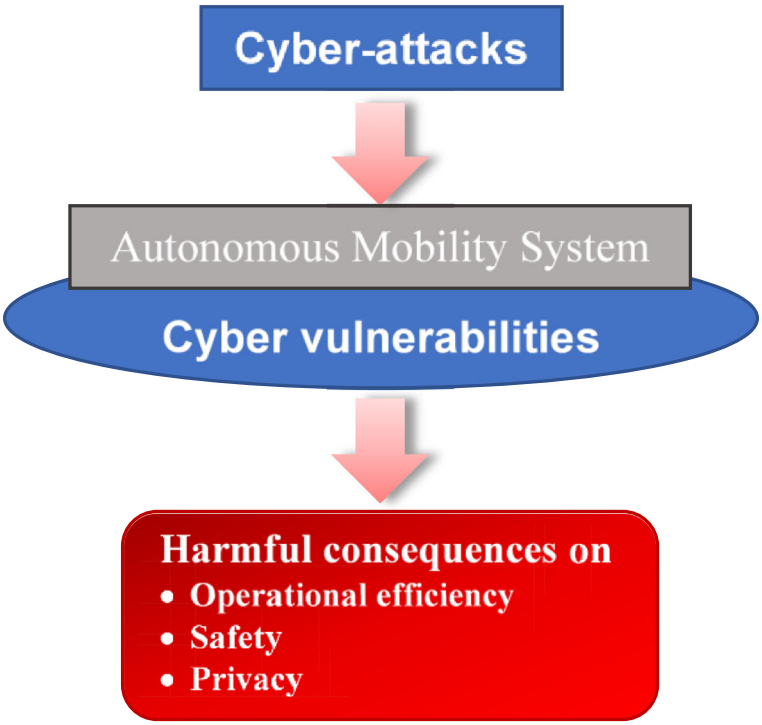

Fig. 4 Cyber-attacks, vulnerabilities, and harmful consequences of cyber-attacks

cybersecurity issues. The relationship between cyber-attacks, cyber vulnerabilities, and the harmful consequences of the cyber-attacks is shown in Fig. 4.

Many types of cyber-attacks are relevant to AMS. We classify a range of plausible cyber-attacks on AMS based on two criteria. The first criterion is whether an attack is more likely for a single AV or for a system. Vehicle-level attacks target functions and devices such as the camera, radar instruments, and internal communication within an AV. By contrast, system-level attacks aim at the sensing, control, and communication infrastructure (e.g., road sensors, traffic lights, and wireless Internet servers) that serves AVs in an area or a type(s) of AVs. Note that aggregating vehicle-level attacks do not necessarily make up a system-level threat because the points of vehicle-level attacks are individual AVs, whereas the points of system-level attacks are not individual AVs but the infrastructure that supports operations and communications of AVs.

The second criterion for cyber-attack classification is whether an attack is active or passive. An active cyber-attack is highly malicious, aggressive, and blatant, attempting to negatively alter the communications and/or operations of AVs. AMS operator(s) will be able to detect once the attack is successful and react immediately. By contrast, a passive cyber-attack employs non-disruptive and covert methods. As a result, no immediate harmful consequence in altering AMS communications and operations. Passive cyber-attacks are often about gathering AV operation/communication data and less likely to draw attentions from AMS operators.

Below we provide brief descriptions of different plausible cyber-attacks to AMS.

Vehicle-level attacks

Gaining steering control of an AV (active attack) Under this attack, an attacker will fully control the motion of an AV toward damaging consequences, for example, by stroking the brake-pedal suddenly or turning the steering wheel of the vehicle to cause crashes. Such malicious attacks, aiming at passenger injury or death, impose very serious safety concerns for AMS. Gaining steering control of an AV can be realized through masquerade attacks (Yagdereli et al. 2015).

Deactivating sensors of an AV (active attack) This type of attacks compromise only the sensor components of a vehicle. Nonetheless, the potential harms could still be considerable. For example, deactivating sensors responsible for detecting surrounding objects (e.g., other AVs, human-driven vehicles, and pedestrians) and lights of the environment will cause traffic accidents. Alternatively, the risks will trigger vehicle safety warnings that results in unexpected stopping of the AV.

Exfiltrating data (active attack) Data exfiltration is a security breach in which data stored in an AV are illegally copied, retrieved, and transferred by attackers. The breach could be through a remote application or a physical access point on the AV. Exfiltrated data can be subsequently used to influence human interactions with AVs and even fool AV users and/or AMS operators to take actions towards nefarious activities (Axelrod 2017).

Rebroadcasting message (active attack) A cyber-attacker can replay a previous message (e.g., an accident alert) to elicit a wanted reaction of an AV (e.g., stroke of a brake pedal). This reaction could force an AV into a vulnerable state (e.g., system reset) or allow the attacker to store information for future attacks. With message rebroadcasting, not only the information integrity but also message authentication and access control of an AV can be compromised.

Introducing incorrect input signals (active attack) If an attacker has access to the vehicle-to-vehicle and/or vehicle-to-infrastructure communication networks of an AV, the attacker can trick the AV into an incorrect action by generating erroneous process information. For example, an accident alert can be sent by an attacker to an AVs to activate the braking-pedal action, creating traffic disruptions in the surrounding area (Yagdereli et al. 2015).

Modifying message (active attack) A cyber-attacker can modify messages either between AVs or between AVs and the AMS operator. The most common means of message modification is through "man-in-the-middle" attacks (Yagdereli et al. 2015). The modification can be delaying the sending/receiving time; inserting/deleting contents; and reordering the sequence that messages are sent. As such, modified messages can direct AVs to take actions wanted by the attacker.

Eavesdropping (passive attack) In eavesdropping, an attacker acquires vehicle movement and communications information by intercepting data traffic to and from an AV. The acquired data are used to plan future active attacks. Data interception often takes

place at devices in the middle of data transmission between AVs and AMS servers. In general, eavesdropping is difficult to detect since it does not cause abnormal data transmissions (Dobran 2019).

Traffic analysis (passive attack) Similar to eavesdropping, traffic analysis does not affect the normal functioning of AV(s). An attacker deducts certain properties of information transactions including duration, timing, and bandwidth that are difficult to disguise in communications. With the deducted information, traffic analysis can be performed to allow an attacker to examine the AV network for other malicious purposes (Yagdereli et al. 2015).

System-level attacks

Denial-of-service (active attack) A common issue for cybersecurity of communication networks, denial-of-service refers to prevention of authorized user access to AMS. A denial-of-service attack can involve malicious coding and message spamming that absorb all available bandwidth, making communications between AVs and infrastructure unavailable. The AMS communications network will be infected by malicious software or by the attacker constantly sending packets to AMS server ports to jam needed communications for normal AV functions such as routing, warning, and spatial sensing.

Interrupting communications (active attack) A cyber-attacker interferes with communications between the control components of an AMS. By issuing a data request that causes the control systems to obstruct the normal processing sequence of the systems to respond to the request, this interference undermines the stability of routine communications and therefore operations of AMS (Kisner et al. 2010; Kisner 2009). Such disruptions, once detected, will prompt the AMS operator to reduce or even cease provisions of mobility service in order to recover or switch to backup communication networks.

Generating incorrect output values or commands (active attack) This type of attacks generates erroneous output values or commands and send them to devices in AMS that enable interaction between cyber and physical components. Consequently, an AMS operator can be misled to take AV routing and dispatching decisions not the best for the current operational status, or even disrupt AMS operations and traffic on the roads.

Collecting AMS operational information (passive attack) This type of attacks attempts to gain access to AMS operation data through eavesdropping AMS servers. Although not disrupting normal functioning of AMS, the information collected can be used to estimate the operational parameters and states of AMS such as distribution, speed, and fueling of AVs, and to help forge more targeted active cyber-attacks in the future.

Enhancing the cyber resilience of AMS

Given the variety of plausible cyber-attacks, making AMS resilient to cyber-attacks is critically important. The premise of doing so is to understand what cyber resilience

means for AMS. Answering this question will build on the understanding of cyber resilience and resilience in general, as is in subsection 4.1. In subsection 4.2, we will examine current practices in strengthening AV cybersecurity, a closely related issue to AMS cyber resilience. Further strategies at both vehicle and system levels to enhance AMS cyber resilience are proposed in subsection 4.3.

Resilience and cyber resilience

Resilience

We start our discussion with the most general definition of resilience. Following the 2019 version of the Merriam-Webster dictionary, resilience is described as the "ability to recover from or adjust easily to misfortune or change". In the academic literature, the concept of resilience is initialized in the context of ecological systems by Holling (1973), who refers to resilience as a system's ability to persist without eventually moving to a different state of behavior when exposed to changes or shocks (Zou et al. 2018). Later, Bruneau et al. (2003) adapt the resilience concept in earthquake engineering, as the ability of a system to resist and absorb the impact of disruptions. Focusing on infrastructure systems, the definition of resilience is enriched by Faturechi and Miller-hooks (2014) who argue that resilience accounts for possible interventions that help returning system performance to near pre-disruption levels. The authors stress the importance of resilience measures in quantifying the potential benefits of pre-disruption mitigation actions for increasing the system's ability to cope with disaster impact, as well as post-disaster adaptive actions that aim to restore system functionality. Another widely-used definition of resilience is from the US National Academy of Science (2012), which relates resilience to the ability of a system to plan for, absorb, recover from, and more successfully adapt to adverse events.

While the definitions/descriptions of resilience vary in emphasis depending on the application context, resilience covers two essential aspects: 1) preparing a system before disruptions; and 2) recovering the system after disruptions occur. The preparation aspect can be alternatively interpreted as enhancing the resistance of a system to attacks. The aim of implementing a comprehensive resilience plan, therefore, is to reduce the potential damages caused by attacks through resistance and enhance fast recovery (Linkov et al. 2013). This two-aspect view is echoed by Zhou et al. (2019), who focus on transportation systems resilience and conclude that all resilience definitions for transportation systems take the following two perspectives: i) the ability to maintain the system functionality under disruptions; and ii) the time and resources required to restore performance after disruptions. As shown in Fig. 5, the first perspective is related to a disruption phase, beginning from the occurrence of a disruption and ending when the system performance reaches the minimum level. In this phase, robustness and redundancy of system functionalities are key to minimize the consequence of disruptions. The second perspective is associated with a recovery phase. When it starts, system performance is expected to improve, till return to the original performance level which means full recovery. This phase usually takes long time than the disruption phase. The abundance and optimal and speedy use of resources are critical to recovery.

Cyber resilience

The general definition of resilience needs to be adapted when resilience specifically addresses cyber-attacks. However, very limited definitions exist for cyber resilience. Linkov and Kott (2019) adapt the resilience definition by the US National Academy of Science and define cyber resilience as the ability of a cyber-physical system to prepare, absorb, recover, and adapt to adverse effects of events associated with cyber-attacks. One can replace "cyber-physical system" by "AMS" if AMS cyber resilience is to be specifically defined.

Compared to other types of resilience, cyber resilience exhibits three particularities. First, the cyber-physical system performance is likely to plummet to a low value shortly after a cyber-attack begins. This is due to the fact that cyber-attacks will be realized through communication networks, often very fast compared to natural processes (e.g., a wildfire or a flood). On the other hand, it may take some time for the consequences of a cyber-attack on the physical system to appear and grow. For instance, when an attack introduces incorrect input signals to prompt a few AVs to brake, the resulting traffic jam will gradually grow from the locales of the attacked AVs to larger networks.

The second particularity of cyber resilience lies on the greater uncertainty of cyber-attacks in attacking forms and techniques which are constantly evolving. Consequently, the traditional approach to predict future attacks based on past experience of similar situations becomes less effective. Collier et al. (2014) highlight that the dynamic and fast development of different types of cyber-attacks makes it impossible to maintain an exhaustive library of possible attack surfaces in the cyber domain. Moreover, the evolving possible surfaces of cyber-attacks adds to the difficulty in ranking and prioritizing the importance of each attack and corresponding mitigation strategies.

The third particularity is about strategies to enhance cyber resilience. Cyber resilience deals with connected complex systems involving hardware, software, and sensing components. In comparison to natural disasters, the smart nature of cyber-attackers

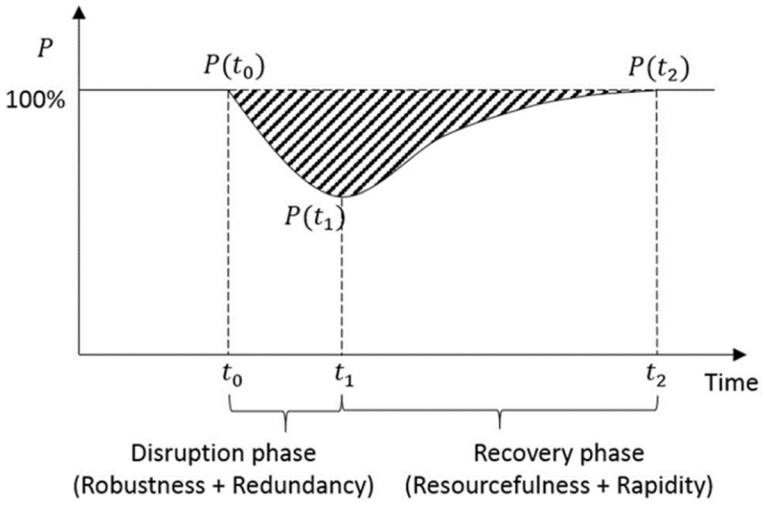

Fig. 5 Decomposing resilience into disruption and recovery phases, where *P* denotes performance (Source: Zhou et al. 2019)

places another layer of complexity for cyber resilience enhancement. Cyber-attackers have the flexibility to attack either part of a system or use more sophisticated attacking methods to cause deeper and broader consequences. Not surprisingly, strategies for resilience enhancement in the cyber world are more varied than strategies dealing with physical system resilience.

Any enhancement of cyber resilience must be built on solid assessment of cyber resilience, which is still at an infant stage. Linkov and Kott (2019) argue that the assessment should draw ideas from the general resilience literature in which two primary approaches have been developed: metric-based and model-based (Fig. 6). The metric-based approach uses metrics of individual properties of system functions to assess the overall performance of a system. For instance, one metric for AMS cyber resilience, following the idea of Hallegatte et al. (2019), can be the ratio of unfulfilled rider trips to the number of malfunctioning AVs for a period starting from the outset of a cyber-attack. For this metric, the number of unfulfilled rider trips represents the loss of system functionality. The number of malfunctioning AVs captures the loss of assets. Intuitively, a lower metric value corresponds to greater cyber resilience.

The model-based approach employs system configuration models and performs scenario analysis to predict system evolution before, during, and after an attack. This approach requires knowledge of the critical functions of the system, temporal patterns of the system, thresholds, and system memory and its learning process (Linkov and Kott, 2019). As an example, the interactions between a cyber-attacker and the AMS operator can be modeled as a sequential attack-defend game. Resilience will be measured based on the expected costs of Nash equilibrium between the attacker and the defender. A lower expected cost means higher AMS cyber resilience.

Both metric-based and model-based approaches have their limitations, however. For the metric-based approach, despite a myriad of research efforts (e.g., Eisenberg et al. 2014; Park et al. 2013) there remains a lack of universally accepted metrics for cyber resilience. The limitation is further compounded in the AMS context by the dearth of

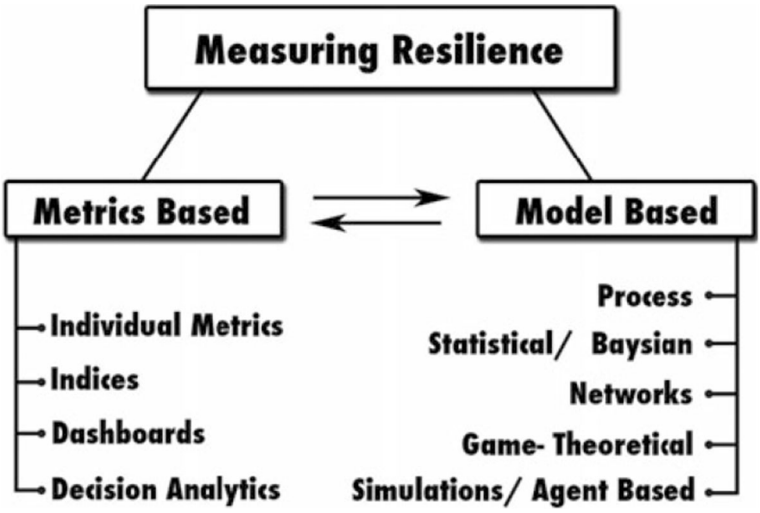

Fig. 6 Metric- and model-based approaches for cyber resilience risk assessment. (source: Linkov and Kott, 2019)

knowledge on the type, probability, and consequence of cyber-attacks on AMS. For the model-based approach, it would be difficult for researchers to acquire all the knowledge about the critical functions of a cyber-physical system, the normal operation patterns of the system, and system adaption after cyber-attacks. Overall, assessment of cyber resilience remains an underexplored area for future research.

Practices related to enhancing cyber resilience

As AMS does not exist, no practice exists for enhancing AMS cyber resilience. On the other hand, cybersecurity as a closely related concept has garnered growing attention. The close relationship between cybersecurity and cyber resilience is not difficult to perceive: a system that is highly cybersecure will not be vulnerable to cyber-attacks. On the other hand, cyber resilience is not just about cybersecurity in that cybersecurity focuses on the pre-attack preparation, whereas cyber resilience involves further post-attack recovery. For example, a system may be highly cybersecure but is not able to recover strongly and quickly once a cyber-attack succeeds. Thus the system is not cyber resilient.

This subsection focuses on reviewing practices towards enhancing AV cybersecurity from two perspectives: 1) developing cybersecurity algorithms, and 2) establishing legislation and guidelines. We note that most practices are undertaken at the vehicle level. The practices involve a wide range of stakeholders including computer scientists/ electrical engineers, transportation systems modelers/ analysts, mobility business executives/engineers, urban planners, policy makers, etc.

Cybersecurity algorithm development

The auto industry has put tremendous efforts in developing algorithms to enhance vehicle cybersecurity (Tuncali et al. 2018; Zhang et al. 2018), to enable vehicles to respond to abnormal situations not experienced before (Pei et al. 2017; Tian et al. 2018). These situations could well be signals of cyber-attacks. By training cybersecurity algorithms to recognize and respond to the situations, the ability of AVs to withstand cyber-attacks will be enhanced. Also, after recognizing a probable cyber-attack situation, an offset action is to have a human driver override autonomous driving (Enache et al. 2009; Katzourakis et al. 2015; Fraedrich and Lenz 2016), e.g., a controller in the AMS traffic management center takes over driving of an affected AV, or a "take-over" request is generated which prompts the rider inside the AV to take control of the vehicle (Guo et al. 2019). To do so, an adequate design of a shared steering control framework, transition functions, and relevant algorithms is of critical importance.

Artificial intelligence particularly deep neural networks has been the prevalent technique for developing cybersecurity algorithms. However, at this moment data for algorithm training is limited which suggests that failures to cope with unrecognized cyber-attacks can occur. This is because traditional, manual collection of data from tests or unguided simulations to identify cyber-attacks would be prohibitively expensive (Karapathy 2017; Sculley et al. 2014). Instead, machine-based testing methodologies are being developed toward automatically detecting erroneous behaviors of AVs (Tian et al. 2018). Given that the attacking forms and techniques are constantly evolving,

detecting all abnormal situations tied with cyber-attacks is still a daunting if not impossible task even with the machine-based testing methodologies.

The research and development efforts for cybersecurity algorithm development goes beyond the auto industry. In the US, the National Highway Traffic Safety Administration has established a department for research on safety, security, and reliability of connected and electronic vehicle systems. An Electronic Council is set up in the agency to enhance collaboration on and alignment of research related to vehicles and cybersecurity (McCarthy et al. 2014). Besides algorithm development, government agencies are also making endeavors in cybersecurity standard development, cyber risk assessment, cybersecurity test, and enforcement efforts.

Legislation and guidelines

National and subnational governments are playing active roles in enacting legislations and introducing guidelines to address cybersecurity issues arising from future AVs as well as today's vehicles. In the US, the federal government has recently passed the SPY Car Act (2017) to address vehicle cybersecurity risks. The Act includes considerations to guard against the hacking of vehicles, such as requiring penetration testing to evaluate vehicle resilience to hacking and separating critical and non-critical software systems. In addition, the Act provides specifications to ensure security of collected information in vehicle electronic systems while the data are on the vehicle, in transit from the vehicle to a different location, or in any offboard storage. This Act requires vehicles to have the capability to detect, prevent, and report attempts to hijack the control of the vehicle and capture the stored data (Lim and Taeihagh 2018; Taeihagh and Lim 2019).

Specific for AVs, the U.S. National Highway Traffic Safety Administration has published a non-mandatory document to facilitate integration of automated driving technologies that encourage the "development of systems that guard against cyber-attacks" (NHTSA, 2017). The document provides recommendations for planning cyber incident responses, developing cyber vulnerability disclosure and reporting policies, and publishing Voluntary Safety Assessment letters. One purpose of this guideline is for standardization, i.e., encouraging entities to design AV systems in compliance with standards established by stakeholder organizations such as the Automotive Information Sharing and Analysis Center, the Society of Automotive Engineers, and auto manufacturer associations (NHTSA, 2017).

At the subnational level, a rule is drafted by the California Department of Motor Vehicles that requires auto manufacturers to certify the ability of their manufactured AVs to detect and react to cyber-attacks according to industry standards (Cal DMV, 2018). The state of Massachusetts has introduced a state bill authorizing the state Department of Consumer Affairs and Business Regulation to implement regulations consistent with federal regulations to protect personal information and data collected by an Internet-of-Things device, which includes AVs (Senate Bill 179, 2017). Pennsylvania's bill makes recommendations for AV testers to provide proof that cybersecurity precautions are taken. Immediate notification of cybersecurity intrusion attempts is required between AV testers and the Pennsylvania Department of Transportation (PennDOT, 2016; Senate Bill 427 2017). Many other states in the U.S., such as Georgia, Michigan, and Texas, have also enacted legislation to address cybersecurity

for larger systems inclusive of AVs (Senate Bill 315 2018; Senate Bill 632, 2017; Texas Cybersecurity Act 2017).

Plausible strategies to enhance AMS cyber resilience

Consistent with the discussions on cyber-attacks and cyber resilience, we argue that plausible strategies to enhance AMS cyber resilience should consider both vehicle and system levels. Vehicle-level strategies are expected to be implemented during AV design and manufacturing, while system-level strategies will focus on the planning and operation of AMS.

Vehicle-level strategies

Auto manufacturers can mitigate the negative impact of cyber-attacks on AVs by adopting a layered approach (GAO, 2016). In vehicle design, cyber-physical networks in a vehicle can be separated by artificial layers. For instance, one can create an engine control unit layer, an in-vehicle communication network layer, and an external interfaces layer. The layer creation will involve technologies such as gateways, firewall, message authentication and encryption, and intrusion detection and prevention systems (Fig. 7). During vehicle manufacturing, several practices can be further considered to identify and mitigate AV cyber vulnerabilities, including: 1) developing over-the-air update capabilities for AV software and firmware; 2) conducting risk assessment and attack testing; and 3) creating domain separation for in-vehicle networks. For the last one, mission- and safety-critical components in an AV can be separated from non-critical components, with limited connectivity to external networks through a few specific communication channels (GAO, 2016; ITF, 2018).

Another vehicle-level strategy is to equip an AV with the ability to continuously monitor its conditions and potential attacks independent of external communications. This ability will reduce the reliance of a vehicle on vehicle-to-vehicle and vehicle-to-infrastructure networks, and ensure prompt triggering of emergency response as soon as a failure is detected. The strategy can include devising an independent procedure for data collection and processing, and activate self-sustained vehicle control whenever external communications are disrupted. For instance, an AV can be designed such that it always compares the information received from surrounding environment with the information collected and processed from its sensing instruments. If a significant

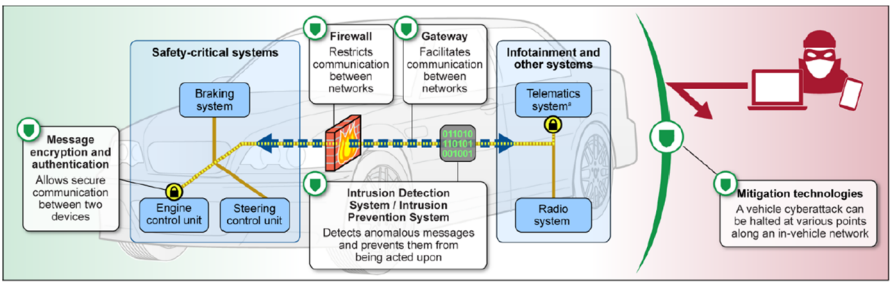

Fig. 7 Illustration of a layered approach to enhance AV cyber resilience (source: GAO, 2016)

inconsistency is detected, an appropriate protocol will be triggered to let the AV rely on its own data for future maneuvering.

System-level strategies

From the perspective of transportation systems planning and operations, three strategies that entail the fundamental concepts for resilience enhancement can be considered: 1) maintaining redundancy, 2) providing diversity, and 3) controlling propagation (Linkov and Kott, 2019). The first strategy pertains to maintaining redundancy in transportation capacity, which can be realized by: 1) operating an AV fleet size larger than the minimum necessary to meet day-to-day travel demand; 2) coordinating the operations of AVs with other modes, especially public transportation. The question of how much redundancy is important. A larger fleet contributes to greater AMS cyber resilience by mitigating the potential loss when a cyber-attack disables the operations of a given number of AVs in the system. However, a larger AV fleet means greater capital and operating cost. To determine the optimal fleet size, careful economic analysis must be performed to quantify the tradeoff between increased capital and operating cost due to redundancy under normal conditions and cyber resilience benefits under cyber-attacks.

It should be noted that some cyber-attacks such as denial-of-service can be immune to an increase in AV fleet size, because the whole AMS will be affected. In such cases, providing alternative transportation modes independent of AMS will be particularly important. An obvious candidate is public transportation. While some argues that AMS would ultimately eliminate today's human-operating transit systems, the claim may be less valid under attack situations. Transit can provide valuable backup capacity to move disrupted AV travelers under cyber-attacks. As such, the possibility of cyber-attacks provides a valid argument for preserving an independent public transportation system in the future even after AMS takes place.

For the second strategy, diversity is realized by maintaining a separate road network for AVs that is free of connectivity. When AVs are using this network, they can only use their automation capability, with no communications between vehicles or between vehicles and infrastructure. AVs would operate like conventional vehicles except that the movement of each AV will rely only on information collected by the AV's own sensing instruments. This strategy aims to make AMS resilient to cyber-attacks on communication networks. For example, if a distributed denial-of-service attack occurs which can affect communications between AVs and the infrastructure serving the AVs, the AMS operator can divert AVs from the normal road network to this separate network.

Maintaining a separate network, however, begs careful planning of the network. This network may be a newly built one but will be costly. Alternatively, one can dedicate part of the existing road system to only conventional vehicles under normal conditions, and to both conventional vehicles and AVs when a cyber-attack occurs. The size and connectivity of this separate network must be judiciously determined by accounting for many factors such as travel demand, overall road network intensity and capacity, and mode share between AVs and conventional vehicles. Similar to the strategy of maintaining redundancy, this strategy should strike a balance between the cost of preserving the network under normal conditions and the benefits of the network in serving travel demand under cyber-attacks.

The third strategy is deploying different sub-autonomous mobility systems rather than a single homogeneous AMS. Between two subsystems, only limited data exchange and connections are allowed so that when a cyber-attack incurs to one subsystem, its negative consequences are contained in the subsystem while other subsystems have high probability of retaining normal functionality. An option to implement this strategy could be using a distributed ledger technology, known as private blockchain, which stores data in a decentralized fashion to maintain security (Mollah et al. 2020; Marvin 2017; Noyes 2016). The idea is similar to the vehicle-level strategy of creating separation in subsection 4.3.1. One way to create subsystems is to have an AMS operator run independent sub-fleets, or mandate competing AMS operators. While market competition is known to benefit AMS users by reducing service price, introducing competing subsystems in AMS brings the additional benefit of enhancing cyber resilience of the overall AMS. The disruption and recovery efforts would be smaller than if the attack spreads over the entire AMS.

Conclusion and future research

The increasing cyber connectivity of vehicles and between vehicles and infrastructure will drastically reshape the way humans move in the coming decades. While the advent of connected mobility—along with the coupled trend of vehicle automation—is expected to benefit travelers and the society by smoothing traffic, improving rider convenience, and reducing accidents, the augmented cyber components in connected and autonomous vehicles and related infrastructure also give rise to the issue of cyber-attacks to the transportation system and how the system can be more resilient to such attacks. It is believed that malicious acts to exploit connected and autonomous vehicles is only a matter of time and will increasingly become a prominent issue in the future of our society.

In view that little attention has been paid to transportation cyber resilience and autonomous vehicles are likely to dominate in the future mobility system, this paper takes a forward-looking approach looking into cyber resilience of AMS. A first-of-its-kind investigation on this topic with a comprehensive literature review is offered. In the investigation, we start by discussing the cyber components and plausible AMS operation scenarios. Then a considerable amount of efforts is devoted to identifying possible cyber-attacks to AMS at both vehicle and system levels. Building upon the literature of resilience and cyber resilience, the discussion moves to the concept of AMS cyber resilience and exploring existing practices to enhance AV cybersecurity, a concept intimately related to AMS cyber resilience. A number of strategies are subsequently investigated toward enhancing AMS cyber resilience. At the vehicle level, creating layers and separation to reduce cyber component connectivity and deploying an independent procedure for data collection and processing are important in vehicle design and manufacturing. At the system level, recommended strategies include keeping redundancy in transportation capacity, maintaining a separate road network, and deploying different sub-autonomous mobility systems. To quantitatively assess the benefits of these strategies, more elaborate, modeling-based research is needed.

As AMS differs from today's transportation system only by the extent of connectivity and automation and the shift from human-driven to autonomous mobility is going

to be gradual, today's transportation can also be informed by the findings, insights, and recommendations obtained in this paper. We hope that the efforts presented in the paper makes a start toward greater understanding cyber resilience of AMS and connected transportation in general. More in-depth investigations can be stimulated in this important but still underappreciated area for a better future of human mobility.

Acknowledgments The research presented in this work was funded by the World Bank Group.

Availability of data and material Not applicable.

Code availability Not applicable.

Funding This paper is funded by the World Bank group.

Declarations

Conflicts of interest/competing interests None.

References

Axelrod CW (2017). Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In systems, applications and technology conference (LISAT), 2017 IEEE Long Island (pp. 1-6). IEEE

Center for Sustainable Systems (2018). Autonomous Vehicles Factsheet. Center for Sustainable Systems, University of Michigan. Pub. No. CSS16–18

Cisco (2019). What Are the Most Common Cyberattacks? Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. (accessed on 22.05.2019)

Collier ZA, DiMase D, Walters S, Tehranipoor MM, Lambert JH, Linkov I (2014) Cybersecurity standards: managing risk and creating resilience. Computer 47(9):70–76

Consumer Watchdog (2019). Kill switch: Why connected cars can be killing machines and how to turn them off. Available at: https://www.consumerwatchdog.org/report/kill-switch-why-connected-cars-can-be-killing-machines-and-how-turn-them (accessed 10.29.2019)

Cokyasar T, Larson J (2020) Optimal assignment for the single-household shared autonomous vehicle problem. Transp Res B Methodol 141:98–115

Deloitte (2016). The future of mobility: what's next? Available at: https://www2.deloitte.com/content/dam/insights/us/articles/3367_Future-of-mobility-whats-next/DUP_Future-of-mobility-whats-next.pdf (accessed 02.02.2019)

Department of Motor vehicles (2018). Modified Express Terms Title 13, Division 1, Chapter 1 Article 3.8—Deployment of Autonomous Vehicles—Deployment of Autonomous Vehicles; State of California Department of Motor Vehicles: Sacramento, CA, USA, 2018

Dobran J (2019) 17 types of cyber-attacks to secure your company from in 2019. Phoenixnap. Available online at: https://phoenixnap.com/blog/cyber-security-attack-types (accessed on 05.23.2019)

Eisenberg DA, Linkov I, Park J, Bates ME, Fox-Lent C, Seager TP (2014) Resilience metrics: lessons from military doctrines. Solutions 5(5):76–87

Enache NM, Netto M, Mammar S, Lusetti B (2009) Driver steering assistance for lane departure avoidance. Control Eng Pract 17(6):642–651

Faturechi R, Miller-Hooks E (2014) Measuring the performance of transportation infrastructure systems in disasters: a comprehensive review. J Infrastruct Syst 21(1):04014025

Fraedrich, E., & Lenz, B. (2016). Societal and individual acceptance of autonomous driving. In autonomous driving (pp. 621–640). Springer, Berlin, Heidelberg

Government Accountability Office (GAO) (2016). Vehicle cybersecurity: DOT and industry have efforts under way, but DOT needs to define its role in responding to a real-world attack. Available at: https://www.gao.gov/assets/680/676064.pdf (accessed 01.29.2019)

Guo C, Sentouh C, Popieul JC, Haué JB (2019) Predictive shared steering control for driver override in automated driving: a simulator study. Transport Res F: Traffic Psychol Behav 61:326–336

Hallegatte S, Rentschler J, Rozenberg J (2019) Lifelines: the resilient infrastructure opportunity. World Bank Report

Holling CS (1973) Resilience and stability of ecological systems. Annu Rev Ecol Syst 4(1):1–23

International Transportation Forum (ITF) (2018) Corporate partnership board report. Safer Roads with Automated Vehicles. ITF/OECD

Karapathy A. (2017) Software 2.0. Available online at: https://medium.com/@karpathy/software-2-0-a64152b37c35. Accessed on: 2019-05-13

Katzourakis DI, Lazic N, Olsson C, Lidberg MR (2015) Driver steering override for lane-keeping aid using computer-aided engineering. IEEE/ASME Trans Mechatron 20(4):1543–1552

Kisner RA (2009) Design practices for communications and workstations in highly integrated control rooms. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research

Kisner RA, Manges WW, MacIntyre LP, Nutaro JJ, Munro JK, Ewing PD, ... Olama MM (2010) Cybersecurity through real-time distributed control systems. Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30

Lim H, Taeihagh A (2018) Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. Energies 11(5):1062

Linkov I, Eisenberg DA, Plourde K, Seager TP, Allen J, Kott A (2013) Resilience metrics for cyber systems. Environ Syst Decisions 33(4):471–476

Litman T (2018) Autonomous vehicle implementation predictions: implication for transport planning. Victoria Transport Institute, available at: https://www.vtpi.org/avip.pdf (accessed 02.05.2019)

Marvin R (2017) Blockchain: the invisible technology That's changing the world. PCMag, available at: https://au.pcmag.com/enterprise/46389/blockchain-the-invisible-technology-thats-changing-the-world (accessed 20 January 2021)

Masoud N, Jayakrishnan R (2017) Autonomous or driver-less vehicles: implementation strategies and operational concerns. Trans res part E logistics trans rev 108:179–194

McCarthy C, Harnett K, Carter A (2014) A summary of cybersecurity best practices (no. DOT HS 812 075). United States. National Highway Traffic Safety Administration

Mollah MB, Zhao J, Niyato D, Guan YL, Yuen C, Sun S, Lam KY, Koh LH (2020). Blockchain for the internet of vehicles towards intelligent transportation systems: a survey. IEEE Internet Things J, 1–28

National Academy of Sciences (2012). Disaster resilience: a national imperative. Available at: http://www.nap.edu/catalog.php?record_id=13457 (accessed 01.31. 2019)

National Highway Traffic Safety Administration. (2017). Automated driving systems 2.0: A vision for safety. Washington, DC: US Department of Transportation, DOT HS, 812, 442

Noruzoliaee M, Zou B, Liu Y (2018) Roads in transition: integrated modeling of a manufacturer-traveler-infrastructure system in a mixed autonomous/human driving environment. Trans Res Part C Emerg Technol 90:307–333

Noruzoliaee M, Zou B (2021) One-to-many matching and section-based formulation of autonomous ridesharing equilibrium. Transportation research part B: methodological, under review

Noyes C (2016) Bitav: fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405

Park J, Seager TP, Rao PSC, Convertino M, Linkov I (2013) Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Anal 33(3):356–367

Pei K, Cao Y, Yang J, Jana S (2017) Deepxplore: automated whitebox testing of deep learning systems. In proceedings of the 26th symposium on operating systems principles (pp. 1-18). ACM

Pennsylvania Department of Transportation. (2016) Pennsylvania autonomous vehicle testing policy: Final draft report of the autonomous vehicle policy task force. Available at: https://www.penndot.gov/ProjectAndPrograms/ResearchandTesting/Documents/AV%20Testing%20Policy%20DRAFT%20FINAL%20REPORT.pdf (accessed 12 June 2019)

Sculley D, Holt G, Golovin D, Davydov E, Phillips T, Ebner D, ... & Young M (2014) Machine learning: The high interest credit card of technical debt

Senate Bill 315. 2018. General Georgia Assembly. Available online: http://www.legis.ga.gov/ legislation/en-US/Display/20172018/SB/315 (accessed on 12 June 12, 2019)

Senate Bill 427. Regular Session. Pennsylvania, U.S., 2017. Available online: https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2017&sessInd=0&billBody=S&billTyp=B&billNbr=0427&pn=0396 (accessed on 12 June 2019)

SPY Car Act (2017). 115th Congress. United States of America, 2017. Available online: https://www.congress.gov/bill/115th-congress/senate-bill/680/text (accessed on 12 April 2019)

Taeihagh A, Lim HSM (2019) Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transp Rev 39(1):103–128

Texas Cybersecurity Act. 2017. Available online: https://capitol.texas.gov/tlodocs/85R/billtext/pdf/HB00008F.pdf#navpanes=0 (accessed 12 June 2019)

Tian Y, Pei K, Jana S, Ray B (2018) Deeptest: automated testing of deep-neural-network-driven autonomous cars. In proceedings of the 40th international conference on software engineering (pp. 303-314). ACM

Tuncali CE, Fainekos G, Ito H, Kapinski J (2018) Simulation-based adversarial test generation for autonomous vehicles with machine learning components. In 2018 IEEE intelligent vehicles symposium (IV) (pp. 1555-1562). IEEE

Yagdereli E, Gemci C, Aktaş AZ (2015) A study on cyber-security of autonomous and unmanned vehicles. Journal Defense Mod Simul 12(4):369–381

Zhang M, Zhang Y, Zhang L, Liu C, Khurshid S (2018) Deeproad: Gan-based metamorphic autonomous driving system testing. arXiv preprint arXiv:1802.02295

Zhou Y, Wang J, Yang H (2019) Resilience of transportation systems: concepts and comprehensive review. IEEE Trans Intell Transp Syst 20:4262–4276

Zou B, Rockne KJ, Vitousek S, Noruzoliaee M (2018) Ecosystem and transportation infrastructure resilience in the Great Lakes. Environ Sci Policy Sustain Dev 60(5):18–31

Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, Von Winterfeldt D (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake spectra 19(4):733–752

Linkov I, Kott A (2019) Fundamental concepts of cyber resilience: Introduction and overview. Cyber resilience of systems and networks. Springer, Cham, pp 1–25