Investigating the Inertia in the Regulation of Vehicle Cybersecurity by Applying a Nontraditional Methodology

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Goutham Subramanian Thiagarajan

Spring 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

Motor vehicles have been the most common form of transportation for over a century. Given the utter dependence of modern society on motor vehicles, it is imperative that future vehicle designs prioritize cybersecurity. The computerization of vehicles has greatly improved the quality of life for drivers and passengers with safety features and assistive technologies. At the same time, the modernization of automobiles has led to them becoming cyber-physical systems (CPSs), which are integrations of computation, networking, and physical processes. However, a CPS requires cybersecurity that is resilient, promotes privacy, protects against malicious attacks, and detects intrusion (Ptolemy Project, 2019, n.p.). Automobiles have become targets for cyberattacks as they become increasingly connected. Possible vehicle cybersecurity attacks can be disruptive as they include engine shutdowns, disabled brakes, and locked doors (Eiza & Ni, 2017, p. 45). Thus, potential consequences range anywhere from minor inconveniences to injuries or worse. While there does exist literature on CPSs, it is unclear exactly how issues of cybersecurity manifest themselves in transportation systems. My deliverable for STS research will be a better understanding on what the entities involved in vehicle cybersecurity are doing, if anything, to maximize public safety.

This paper will apply multiple frameworks to the field of vehicle advancement to approach a resolution. The first framework will apply routine activity theory (RAT) to examine the situations of cybercrimes. The second framework will examine different risks associated with computerized vehicles. The last framework will synthesize literature about cybersecurity to determine how vehicles conform to general principles of cybersecurity and how they do not. These three frameworks will be amalgamated with the intent of applying frameworks not traditionally associated with vehicle cybersecurity to vehicle cybersecurity so that new

discoveries can be yielded. In this paper, I argue that the continued computerization of motor vehicles should be cautiously monitored as to reduce the possibility of future cybersecurity attacks because minimizing the human element may very well be replacing one problem with another.

Part 1: Systems Intended to Enhance Comfort and Safety Are Susceptible to Tampering

For much of the past century, vehicles were machines that were separate and wholly mechanical with the sole function of transportation. As concepts such as the Internet of Things grow in popularity, "consumers increasingly demand a seamless connected experience in all aspects of their lives including driving" (Eiza & Ni, 2017, p. 45). But it should be noted that the ever-increasing desire of society for technological enhancement and connectivity in all facets of modern life means that devices and equipment are being used for functions that they were not intended for. A pervasive example of such a device is a smartphone, which more often serves purposes such as games and social media than that for which they were intended: making phone calls. Smartphones, which themselves have only become commonplace over the past decade, are already integrable with most modern models of cars.

Cyber-physical transportation systems in some ways have existed for a long time but new possibilities are emerging such as autonomous vehicles (AVs), which sense the environment and move safely with little if any human input (Taeihagh and Lim, 2017, p. 105). AVs appear to be gaining acceptance as 78% in a survey of 5400 people believed that autonomous cars were either better drivers than humans or would be within the next ten years (Mircică, 2019, p. 45). Features such as adaptive cruise control, lane management, collision avoidance, and parking assistance have increased safety by reducing the capacity for human error, a major cause of accidents. Central to vehicle enhancement is a focus on connectivity as even non-autonomous vehicles are

now “controlled by hundreds of electrical control units (ECUs) that form an internal network of devices within the vehicle” (Eiza & Ni, 2017, p. 46). Vehicles are also capable of communicating with each other or with infrastructure, and this system is microcosmic of a connected world. Even though increasing connectivity and autonomy in vehicles potentially leads to greater convenience and functionality, it likely also leads to new cyberthreats.

In a notable incident in July 2015, two researchers demonstrated the feasibility of a cyberattack on an automobile when they hacked into a Jeep Cherokee that was on a highway ten miles away (Greenberg, 2015, n.p.). By exploiting a software known as Uconnect, the researchers were able to remotely control the car functions using a simple third-generation (3G) connection. Using this vulnerability as an attacking entry point, they were able to rewrite the firmware of the adjacent chip in the car’s head unit and disable the brakes, control the steering wheel, and send the vehicle into a ditch (Greenberg, 2015, n.p.). This incident caused the recall of 1.4 million cars (Eiza & Ni, 2017, p. 46). Moreover, it represents a proof of concept that physical access to the car is no longer necessary to hack into it. It would appear that a hacker needs only to be in the communication range of a vehicle to possibly take control of its most critical functions and cause mayhem. For example, simply and unexpectedly deploying airbags in a vehicle driving on a highway represents a lethal cyberattack that could claim lives by causing a crash. Understanding cyberthreat vectors against vehicles can help identify attack entry points. The figure below indicates that common technologies used within cars such as Wi-Fi, Bluetooth, USBs, and GPS are potential attack vectors.

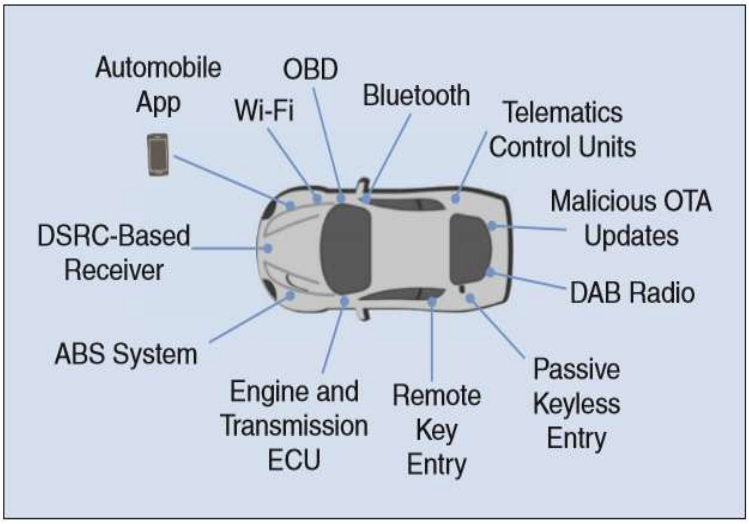

Figure 1. An illustration of the potential vectors of cyberattacks in a car. These include well-known technologies such as Wi-Fi, Bluetooth, and apps as well as lesser-known ones. It also emphasizes that these vectors can be internal or external to the car (Eiza & Ni, 2017, p. 46).

However, the major issue that the field of automotive cybersecurity faces is that to date no road accident has occurred because of a "failure of automobile cyber insecurity" (Schellekins, 2016, p. 307). Furthermore, all reported attacks against vehicles have been carried out by "security professionals in controlled environments" (Kennedy et al, 2019, p.636). This has likely led to a reactive strategy in which solutions are only found to problems that have shown themselves as evidenced by the case of Jeep above. As Golden (2019) notes, there exists a "severe and confusing degree of variance among the industry manufacturers in terms of cybersecurity preparedness" and this indicates that a successful cyberattack on a large scale could have devastating consequences (n.p.).

With regard to potential approaches to resolution, Eiza and Ni (2017) note that it is not feasible to design one security solution for the whole system because ECUs usually come from different vendors (p. 50). Kennedy et al. (2019) additionally views the system from a criminological perspective as they note that connected and autonomous vehicle (CAV) technologies are conducive to creating "a unique criminal opportunity structure" that is linked to

an “illicit actor’s ability to leverage common vehicle technologies, communications systems, user interfaces and modes of communication to gain access to a vehicle’s internal systems” (p. 636). That is to say due to the commonality found across vehicle technologies, a weakness found in one vehicle can likely be found in similar vehicles.

For one, the National Highway Traffic Safety Administration (NHTSA) (2016) recommended a layered approach to cybersecurity with four main focuses: isolating affected subsystems to reduce the effects of a successful attack, using intrusion-detection measures that are real-time, preserving the ability of the driver to control the vehicle after an attack, and using information from previous attacks to evaluate existing protection mechanisms (p. 10). However, it should be noted that the above guidance for best practices is optional and nonbinding and there is no way of ensuring that these recommendations are accepted (Kennedy et al, 2019, p. 643). This is concerning because the NHTSA, which “possesses regulatory authority to develop and enforce safety standards for vehicles, has yet to mandate manufacturer action to secure vehicle control systems against malicious attacks” (Bose et al, 2017, p. 146). The lack of centralized authority and standardization is exposed as there is no body, governmental or regulatory, that “provides information on known threats to vehicles in a single repository” (Kennedy et al, 2019, p. 643). New features are continuously added to vehicles by manufacturers, but cybersecurity should not be neglected given that there are human lives at stake. Thus, the mechanism by which issues of cybersecurity manifest themselves in transportation systems must be elucidated.

One approach to resolution that may be of interest is criminological theory, specifically a routine activities perspective that examines the situations of crimes. Central to this perspective is that the absence of a capable guardian is necessary for most criminal behavior. In this scenario, guardians can consist of automobile manufacturers and relevant component suppliers as it is their

responsibility to secure "cars and their users against the actions of actors who would attempt to gain access to a vehicle, its systems, or data" (Kennedy et al, 2019, p. 633). This theory was not developed with cybercrime in mind but its universality allows for interesting parallels between cybercrime and non-cybercrime. The second framework will examine the major technological risks that accompany computerized vehicles. Varying attitudes towards cybersecurity by the public and regulators are important in shaping the impression of cyber risk in vehicles. The last framework will determine how vehicles conform to general principles of cybersecurity and how they do not by synthesizing literature about vehicle cybersecurity. This literary synthesis can identify the strategies that can be adopted and the emerging responses by regulators to address these risks.

Part 2: Analyzing the Merits and Characteristics of Three Different Frameworks

Routine activity theory (RAT) introduces an unconventional perspective

The first methodology that was pertinent to this research was RAT. RAT is a criminological theory and it should be noted that even though there is little criminological literature to date examining vehicle cybersecurity given its recency as a field, there are clear points where this theory can be applied. In particular, this framework can be used to explore different ways by which vehicle cybersecurity risks can be mitigated or prevented. Unlike traditional models of STS research and analysis, this theory uniquely focuses on crime events by providing "a holistic description of criminal opportunity structures by focusing upon the ways in which motivated offenders, suitable targets, and places conducive to crime interact" (Kennedy et al, 2019, p. 634). Given that this theory was not developed with sociotechnical systems in mind, it could present conclusions that eluded more conventional perspectives. One assumption that will be made for the application of RAT is that the motives for traditional hacks of data and

networks is similar to that for vehicle cyberattacks. Such motives would likely include a desire to cause financial loss or mayhem.

Essential to RAT is the role of guardians, which in this case include but are not limited to automobile manufacturers, or original equipment manufacturers (OEMs), and suppliers. The concept of guardianship allows for roles and responsibilities to be clearly framed. OEMs and suppliers must be guardians because they produce the potential targets of a cyberattack: the hardware and software systems. Thus, they theoretically have the ability to "design-out opportunities for crime as they go about engineering, developing, and deploying the technologies essential to vehicle functioning" (Kennedy et al, 2019, p. 634). RAT is particularly effective because it clearly delineates what is required for a crime to occur as seen in the below figure.

Figure 2. Self-made Venn diagram triangle that illustrates the three necessary elements for a crime (the innermost intersection) to occur according to routine activity theory. If one of the three is removed, then a crime can be prevented so this paper focuses primarily on the bottom-right due to its ability to influence the other two.

In order to reduce ambiguity, it would be prudent to define security with regards to a vehicle. One potential definition of security would be one that emphasizes dependability and intended behavior. In terms of determining current readiness and awareness of cyber risk, understanding the role of victim complacency is key. For example, it must be noted that "there are few, if any,

resources available for automotive owners to identify or mitigate attacks against their vehicles" and this means that security products have yet to be released by auto manufacturers (Kennedy et al, 2019, p. 637). The absence of such products allows attacks to go unobserved, which means that consumer education must be a focus. The lack of such security is conducive to an environment in which consumers may have a minimized perception of the cybersecurity of their vehicles. Thus, the evidence that will be analyzed with respect to RAT will be the current role of guardians and regulatory agencies.

Assessing technological risks can inform public opinion

Another approach involved assessing risk in automobile cybersecurity and determining how it is communicated. Given that public opinion plays a significant role in directing policy and technological development, current attitudes toward technology must be monitored. Viewing such a multidimensional issue through the binary lenses of either optimism or pessimism can lead to a "danger that particularly critical attitudes are easily rejected as non-rational and life-denying" (Kerschner and Ehlers, 2016, p. 140). The goal is to examine and categorize the risks associated with computerized vehicles so that the behavior around innovative technologies can be analyzed using the framework of risk communication by Paul Slovic, a prominent theorist and researcher in the field of risk perception. This framework maintains that informing the public of risk issues is difficult due to a "number of obstacles that have their roots in the limitations of scientific risk assessment and the idiosyncrasies of the human mind" (Slovic, p. 48). One such obstacle is the presentation of complex technical material that may be both uncertain and inherently difficult to understand for the uninitiated. The research findings and conclusions compiled by Slovic can be instrumental in understanding the strengths and shortcomings in the perception of vehicles and their cybersecurity. Slovic also makes the point that risk assessors and

risk managers have attempted to communicate with the public under the false assumption that they and the public "share a common conceptual and cultural heritage in the domain of risk" (Slovic, p. 55). It is undeniable that experts possess more technical knowledge than the people they are trying to communicate to, but members of the public have a basic conceptualization of risk that may be richer because it is their everyday lives that will be affected. These asymmetries can lead to different definitions of risk between the two groups. Focusing too closely on accident probabilities, or the lack of accidents in the case of vehicle cybersecurity, can minimize the problem context.

Using synthesized literature to assess automobile cybersecurity

Synthesizing literature about cybersecurity as an individual discipline and with relation to transportation systems will be helpful in determining how effectively vehicles conform to general principles of cybersecurity. This literary synthesis can not only describe the risks associated with computerized vehicles but also identify and categorize the governance strategies for addressing these risks.

Part 3: Combining the Discoveries Made by Approaching a Comprehensive Resolution

Suggestions revealed by using RAT

Applying RAT reveals that OEMs and suppliers are not traditional actors because they are constrained by legal and structural factors but this does put them in a position to address opportunities for safety due to their direct involvement in the manufacturing of the vehicle. This can be seen by the evidence of specific safety standards such as the inclusion of operational seatbelts and airbags in all vehicles regardless of whether or not they are used responsibly. This can be extended to cybersecurity threats because they are already invested with the responsibilities of a guardian. Kennedy et al (2019) also makes the argument that OEMs and

suppliers have a vested interest in preventing cybercrime against their products because they still own the intellectual property in the systems of the vehicle even though the vehicle itself has transferred ownership to the customer (p. 637). Due to this direct connection between guardians and the target of crimes, OEMs and suppliers should be incentivized at least for the sake of avoiding liability. Liability itself is worth monitoring because organizations may seek to eschew ownership due to corporate risk mitigation strategies if it is possible for another party to assume the risk built in to a product or service. However, such diffusion of responsibility is counterproductive when considering the end goal of proactive cybersecurity. Given how rapidly evolving vehicle technologies are, OEMs must be more communicative with suppliers to ease the integration of systems and components from outside partners.

There are challenges that oppose the implementation of a viable strategy, namely, organizational inertia. The perspective that the issue is the responsibility of someone else can be destructive because this reinforces the tendency to maintain the status quo, which is unsatisfactory in the case of vehicle cybersecurity. In such a scenario, Kennedy et al (2019) suggests that regulatory agencies must also play an active role by galvanizing OEMs and suppliers to take action (p. 637). This could be done by allowing the NHTSA to create and then enforce minimum safety standards to which OEMs and suppliers must adhere as opposed to the current optional guidance.

Hypothesizing technological risks

Identifying the types of risks associated with vehicle cybersecurity can illuminate the areas that OEMs and suppliers must be aware of. The first of these risks is safety. At least 90% of vehicle accidents are estimated to be caused by human error (Taeihagh and Lim, 2019, p.106). Consequently, newer features such as automatic parking and self-driving aim to minimize human

error by phasing out the human element entirely. However, eliminating human error does not eliminate machine error. As autonomous vehicles (AVs) gain more driving experience in the real-world, their performance may improve over time. However, the algorithms that program AVs to respond during unavoidable accidents may lead to moral dilemmas. For example, two possible choices may be either to prioritize the safety of occupants or to achieve a utilitarian outcome that benefits the most people possible. In both scenarios, it is unclear what factors should be taken into consideration when implementing rules to regulate the reactions of AVs.

Similarly, liability is another risk associated with AVs. When humans are in direct control of vehicles, assigning blame is fairly straightforward. However, the dynamic shifts when humans are no longer in control. As discussed previously with RAT, those who design safety systems may now become liable for accidents as it now becomes an issue of product safety. My research indicates that there are currently no legal systems that exist to allocate responsibility among the third parties involved in the design of computerized vehicles and how much of it the human must assume if any. The lack of standardization and concrete criteria for decision-making makes it ambiguous as to the ethical responsibilities of those who design algorithms to respond to crashes.

Another relevant factor is privacy. Much information is processed by computerized cars and there is much uncertainty about informational privacy. For example, ambiguities exist as to "the exact reasons why information is being collected, the types of information being collected, accessibility to the information and the permissible duration of information storage" (Taeihagh and Lim, 2019, p.113). Two major concerns may be the ability to access the location of an AV at any given time or harvest personal information with the intent of conducting surveillance or identity theft in extreme cases.

Cybersecurity threats themselves are also relevant. As discussed previously, there exist multiple points of entry by which hackers could wirelessly control a vehicle. The Jeep Cherokee example that was mentioned in the first part serves as a proof of concept that attacks of malicious intent are not an impossibility. Threats on vehicles are unique in that they have the potential to directly cause casualties unlike standard cybersecurity threats which involve data breaches of and disruptions to faceless organizations such as tech companies, governments, or financial institutions but the parallels between these two types of threats are worth noting.

Discoveries made by reviewing cybersecurity literature

Terminology and precise definitions are integral to this framework. An authoritative definition of cybersecurity defines it as "not necessarily the protection of cyberspace itself but also the protection of those who function in cyberspace" (Haapamäki & Sihvonen, 2019, p. 812). It quickly becomes apparent that cybersecurity is an umbrella term that means more than just information security. Examining existing literature for these more specific terms provides a lens to determine how computerized vehicles conform to general principles of cybersecurity. Literature, both theoretical and empirical, identifies research themes that can be applied to the governance of AVs. These research themes include cybersecurity and information sharing, investments in cybersecurity, the disclosure of cybersecurity activities, and security threats and breaches (Haapamäki & Sihvonen, 2019, p. 808). Information sharing between manufacturers of AVs would be ideal in that it allows for a collaborative effort to be put forth in solving a common issue. However, such a practice might be difficult for manufacturers to accept willingly as sharing relies on them being altruistic and actively sharing private information. Investments in cybersecurity are also relevant because it is unclear how much auto manufacturers should spend in this area. Spending too little runs the risk of neglecting the issue entirely and the novelty of the

field makes an exact determination of expenditure difficult; however, a holistic view that takes into account financial and legal aspects in addition to technical ones may prove most effective. The disclosure of cybersecurity activities by corporations can be a double-edged blade as it makes public that cybersecurity is a priority but this in can return provide incentives for cybercriminals to attack, which will likely increase the possibility of an attack, the development of and effects of which can be seen below.

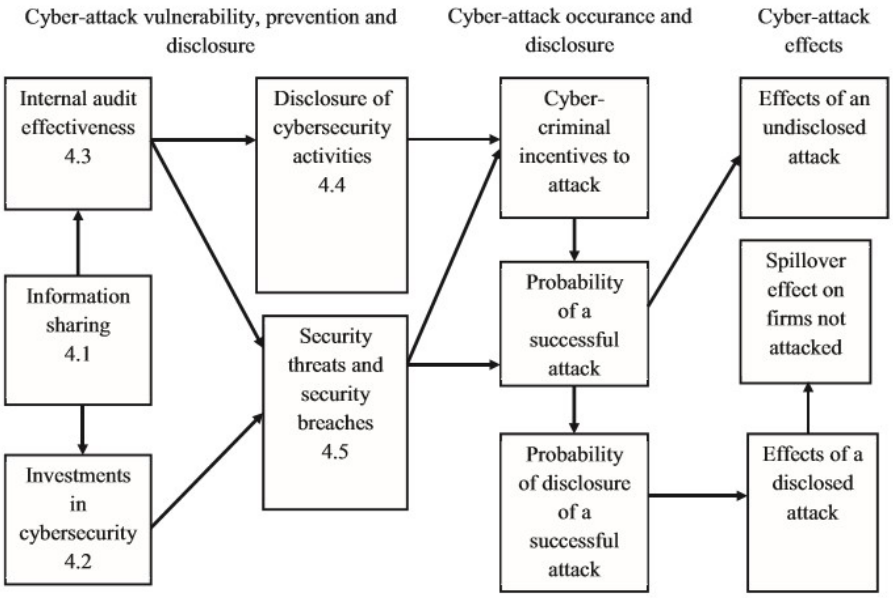

Figure 3. A flowchart of how various cybersecurity research streams are related and the consequences they can bring about. What this paper is most interested are the applications of the research streams (4.1-4.5) due to their assessment of vulnerability, prevention, and most importantly disclosure. (Haapamäki & Sihvonen, 2019, p. 819)

Weaknesses in security can lead to threats and breaches, which can have consequences on not only the affected company but other companies as well. As the figure above shows, it can be deduced that the source of all cybersecurity incidents is the lack or poor quality of information sharing, which was what this section served to investigate the effects of.

Tying these frameworks together

The results of the application of these frameworks can be used to establish various strategies for the governance of computerized vehicles. RAT theorizes that the presence of a

capable guardian is a necessity and this does not appear to be the case around the world. Such a guardian must use various strategies to eliminate risk. Strategies that are oriented around the prevention of risk will likely be more effective than strategies that try to control or tolerate risk, strategies that embrace uncertainty such as adapting reactively, or strategies that involve inaction. Current strategies appear to follow the latter in the United States, which signifies the need for top-down action. A step toward the realization of a risk-preventive strategy is facilitating and encouraging the sharing of valuable information between stakeholder entities.

Conclusion

Modern vehicles are evolving into computers on wheels and this development may bring benefits by minimizing the human element; however, it may be very likely that one problem is being replaced with another. This paper argued that the rate at which motor vehicles are being computerized should be carefully observed as to reduce the possibility of cybersecurity attacks. Using a criminological theory such as RAT introduced a rarely used perspective to investigate the environment of a crime and specifically looked at one of its essential elements: the absence of a capable guardian. Other methods looked at the technological risks arising from computerized vehicles and the application of generalized cybersecurity literature to the field of automobile systems to gauge public reaction and determine how characteristics of traditional cybersecurity can be seen in a nascent area. Thus, the ultimate contribution of this paper was the combination of applying of these three frameworks not typically associated with vehicle cybersecurity to make discoveries that were not previously evident as can be seen in the flowchart below.

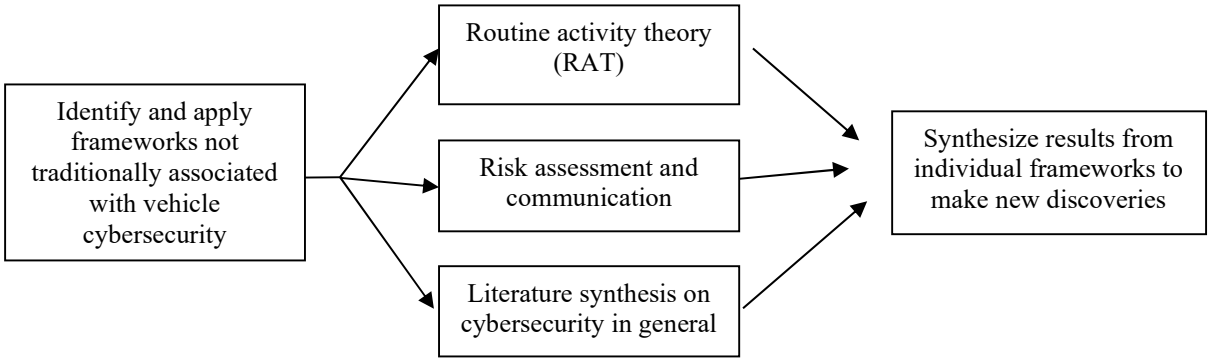

Figure 4. A self-made flow chart that illustrates the intentions of this paper – more specifically, the framework used, why they were selected, and what was done with what was yielded

Tying the results of these frameworks together yielded the first steps to a potential solution that was not evident before. It may be that automobiles are cyber-physical systems that prove too difficult to be reliably and repeatedly hacked but it would be in the best interest of public safety to be better safe than sorry.

Sources

Bose, A., Gilpin, L., Agosti, J., & Dang, Q. (2017). The Veicl Act: Safety and Security for Modern Vehicles. *Willamette Law Review*, *53*(2), 137–159. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=125932678&site=ehost-live&scope=site

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway-With Me in It. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Golden, J. (2019). The Darkening Storm of Cyberterrorism: International Policy Adaptation for Automotive Cybersecurity Regulations. *Jurimetrics: The Journal of Law, Science & Technology*, *59*(3), 267–312. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=137300566&site=ehost-live&scope=site

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in Accounting Research. *Managerial Auditing Journal*, *34*(7), 808 - 834. doi:10.1108/MAJ-09-2018-2004

Eiza, M., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine. 12*(2), 45 - 51. doi: 10.1109/MVT.2017.2669348

Kennedy, J., Holt, T., & Cheng, B. (2019). Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. *Journal of Crime & Justice*, *42*(5), 632–645. https://doi.org/10.1080/0735648X.2019.1692425

Kerschner, C. & Ehlers, M. (2016). A framework of attitudes towards technology in theory and practice. *Ecological Economics*. *126*. 139-151. 10.1016/j.ecolecon.2016.02.010.

Mircică, N (2019). "The Design, Implementation, and Operation of Self-Driving Cars: Ethical, Security, Safety, and Privacy Issues," *Contemporary Readings in Law and Social Justice 11*(2): 43–48. doi:10.22381/CRLSJ11220196

NHTSA (National Highway Traffic Safety Administration). (2016). Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Retrieved from https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

Ptolemy Project. (2019). Cyber-Physical Systems – a Concept Map. Retrieved from https://ptolemy.berkeley.edu/projects/cps/.

Schellekens, M. (2016). Car hacking: Navigating the regulatory landscape. *Computer Law & Security Review*. *32*. 10.1016/j.clsr.2015.12.019.

Slovic, P. (n.d.). Beyond Numbers: A Broader Perspective on Risk Perception and Risk Communication. 48-63. Retrieved from Collab.

Taeihagh A. & Lim H. S. M. (2019) Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, *Transport Reviews*, *39*(1), 103-128, DOI: 10.1080/01441647.2018.1494640