Taylor & Francis
Taylor & Francis Group

Applied Artificial Intelligence
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uaai20

Impact of Factors Influencing Cyber Threats on Autonomous Vehicles

A. Seetharaman, Nitin Patwa, Veena Jadhav, A. S. Saravanan & Dhivya Sangeeth

To cite this article: A. Seetharaman, Nitin Patwa, Veena Jadhav, A. S. Saravanan & Dhivya Sangeeth (2021) Impact of Factors Influencing Cyber Threats on Autonomous Vehicles, Applied Artificial Intelligence, 35:2, 105-132, DOI: 10.1080/08839514.2020.1799149

To link to this article: https://doi.org/10.1080/08839514.2020.1799149

Published online: 09 Dec 2020.

APPLIED ARTIFICIAL INTELLIGENCE
2021, VOL. 35, NO. 2, 105–132
https://doi.org/10.1080/08839514.2020.1799149

Taylor & Francis
Taylor & Francis Group

Impact of Factors Influencing Cyber Threats on Autonomous Vehicles

A. Seetharaman, Nitin Patwa, Veena Jadhav, A. S. Saravanan, and Dhivya Sangeeth

S P Jain School of Global Management

ABSTRACT

Advanced Technologies are transforming the Automotive industry and the pace of innovation is accelerating at a breakneck speed. Autonomous Vehicles (AVs) incorporate many different systems and technologies and their increased computer functionality and connectivity lead to enormous cybersecurity risk. The aim of this research is to explore the significant factors that influence cyber threats on AVs and to examine their level of importance.

Partial Least Squares path modeling was preferred for research studies for its flexible modeling and identifying key drivers. The data analysis was carried out using ADANCO 2.0.1 to develop and evaluate the structural model and the causal relationships between the variables.

Correlation of in-vehicular network vulnerabilities with trust and the correlation between the "workload of the driverless system" with cyber-attacks and cyber threats to AVs are two relations but have not been touched upon in previous studies. In this research, a modified framework is proposed based on the Cyber Cycle and integrated model of Diamond Model of Intrusion Analysis with the Active Cyber Defense Cycle.

Introduction

The advent of Autonomous Vehicles (AVs) creates "Revolution" (shift from human-driving to machine-driving) and "Evolution" (change in definition from "who a driver is" to "what a driver is") (McChristian and Corbett 2016). According to the World Health Organization Report (2013), road traffic accidents are one of the main causes of death among young people worldwide. About 94% of serious road accidents were caused by human distraction [53]. AVs can improve road safety by reducing the number of accidents and other injuries caused by human error (Fitch, Bowman, and Llaneras 2014), reduce congestion, engage in non-driving tasks, better transportation services, efficient land use, and mobility access to people with driving constraints (elderly, disabled) (Anderson et al. 2014). However, there are concerns about the extent of these predicted benefits (Taeihagh and Lim 2018) and about the issues such as privacy, environmental impact, economics and cybersecurity (Shladover,

CONTACT Nitin Patwa nitin.patwa@spjain.org

2015). One of the biggest threats that society expect to face is the Cybersecurity which is less explored and still unknown even among those in the industry (Toews 2016)

Autonomous Vehicles

According to The Society of Automotive Engineers International's Scale of Automation, fully Autonomous Vehicles belong to the Level 5 category. AVs can drive itself with no human intervention and works on a three-phase design called "sense-plan-act" to perceive its dynamic driving environment in real time using sensors, cameras, and navigation systems and make the right driving decisions (Bagloee et al. 2016). AVs are the promising technological change that could reduce the social and monetary costs of accidents [53].

Cyber Threats

A cyber threat is "any event that has the potential to adversely affect people, property (tangible or intangible), organizations or the nation by unauthorized access through an information system" [54]. Cyber-attack can be targeted on any device that is connected to the internet with the malicious aim to disrupt or damage and people's reliance on digital technologies will create more opportunities for cyber-attacks. Cyber-attacks can be Passive (no system damage but eavesdropping to gather information) or Active (more fatal to the system or the entire network). Attackers could be Internal (with authorized system access) or External and with intentional or unintentional purposes (Shladover 2015). The frequency and cost of successful cyber-attacks continue to grow exponentially worldwide (Kamhoua et al. 2015) and rapid advances in cybercrime technology have led to an unprecedented increase in security breaches. World Economic Forum Report in 2018 announced the most serious global risks of 2018 and cyber-attacks were one among the top four.

Cyber Threats on Autonomous Vehicles

Cyber-threats are likely to be a more prominent concern in AVs since they are simply an evolution of modern vehicles and hence inherits its associated cybersecurity issues (Haddrell 2016). Due to their dependence on sensing, communication and artificial intelligence, AVs are attractive targets for cyber-attacks (Shladover, 2015). Threats could be Internal (attacking the in-vehicle systems and communication network) or External (hacking through devices, systems, applications and other technologies connected to the vehicle; for example, remote diagnostic systems, third-party applications) (Haddrell 2016). The attackers could take total or partial control of the vehicle {critical vehicle systems, in-vehicle sensing technologies, and navigation systems}, the

infrastructure or unauthorized access to gain sensitive personal information. Wide range of threat vectors have not yet been fully identified and cyber threats have been a less explored area of research in AVs (Bagloee et al. 2016).

Seven factors that influence cyber threats on AVs have been identified based on the literature review: Socio-cultural, Regulations, Intelligent Transportation Systems, Predictive Measures, Cyber Attacks, in-vehicular Network, and Trust.

Cyber Cycle & Integrated Theory of Diamond Model and the Active Cyber Defense Cycle

In this study, we have used the "Cyber Cycle" theory which states that "*the tussle between hackers and protectors is an unending competition*." Figure 1Cyber attackers wish to maximize the damage to the system while cyber defenders want to minimize it. Attackers scan networks for possible vulnerabilities and develop exploits to attack them. Defenders monitor the network to detect attacks, analyze exploits and deploys security strategy to protect the system. Defender's "detect then mitigate" strategy is highly unstable making systems extremely vulnerable to unknown attacks (McMorrow 2010) (Daly, Endicott-Popovsky, and Wendleberger 2002) (Adams et al. 2013).

The technological capabilities of attackers and defenders have evolved swiftly and in tandem (Mandt 2017). In this study, we will be focusing on the defender's cyber process and we have examined that cyber cycle theory and unified theory of *Diamond Model* and the *Active Cyber Defense Cycle* by (Mandt 2017) can be integrated and applied for cyber threats on AVs. The results of this integration provide a cyber-threat intelligence analysis of attackers and an active cyber-defensive security strategy for the defenders. This is further discussed in the contributions section.

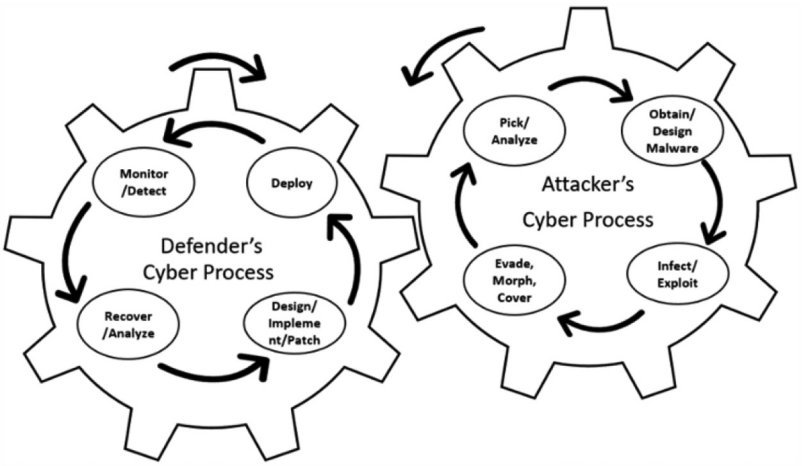


Figure 1. Cyber cycle.

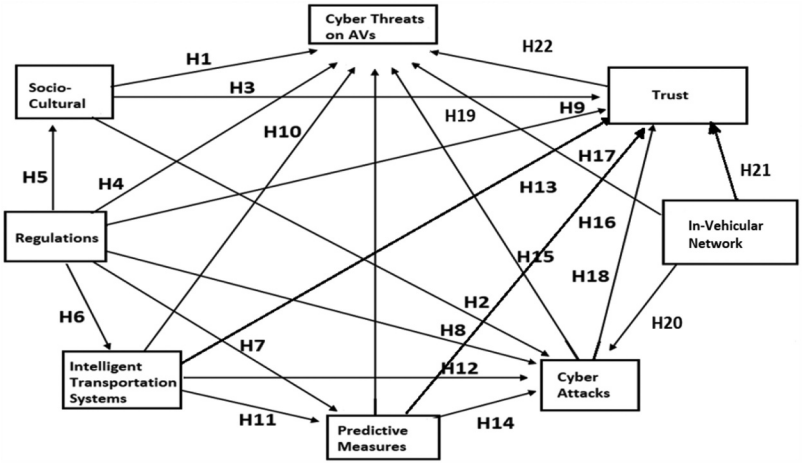
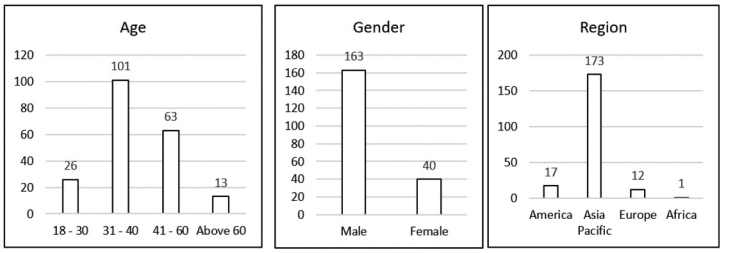


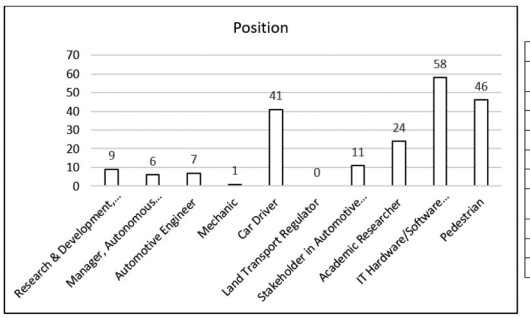
Figure 2. Research framework.



Age	Percentage
18 - 30	12.81%
31 - 40	49.75%
41 - 60	31.03%
Above 60	6.40%

Gender	Percentage
Male	80.30%
Female	19.70%

Region	Percentage
America	8.37%
Asia Pacific	85.22%
Europe	5.91%
Africa	0.49%



Position	Percentage
Research & Development, Autonomous Vehicles	4.43%
Manager, Autonomous Vehicles	2.96%
Automotive Engineer	3.45%
Mechanic	0.49%
Car Driver	20.20%
Land Transport Regulator	0.00%
Stakeholder in Automotive Industry	5.42%
Academic Researcher	11.82%
IT Hardware/Software Engineer	28.57%
Pedestrian	22.66%

Figure 3. Demographics of respondents.

Literature Review

Socio-Cultural Factors

Since the beginning of the 20th century, the automobile has revolutionized our spaces, practices, cultures, and identities by complex linkages (Fraedrich, Beiker, and Lenz 2015). The advent of AVs will have a tremendous impact on our society. Many socio-cultural factors, not technological, seem to be the potential barrier to widespread acceptance of AVs (Bonnefon, Shariff, and Rahwan 2016) which is crucial for the success of AV technology and realize the predicted benefits (Regan 2017). The following three aspects have been identified:

Re-engagement – In the event of system failure or other situations, the process of how efficiently and rapidly the driver takes over control from machine-driving is a key area. The time taken over is likely to be influenced by a combination of traffic density, driver experience and driver engagement in secondary tasks (Zeeb, Buchner, and Schrauf 2015) (Cunningham and Regan 2015).

Workload of Driverless System – According to (Wu and Liu 2007), excessive driving-related information provided to the user might increase the workload and have a negative impact on safety.

Liability issues – Despite AVs perceived benefits, accidents still may occur by its programming (Naughton, 2015). Current AV regulations pertaining to product liability are yet to be updated and it is necessary to provide a framework to determine who or what is to blame or responsible for the accidents for the remedial procedures (Villasenor 2014) (Brodsky 2016) (Glancy 2015).

Regulations

Current laws and regulations pertaining to AVs deal primarily with the authorization of AV testing on the roads. Some US States foster its development without any AV legislation (McChristian and Corbett 2016). The laws regulating the operation of AVs are also reactive and should make progress with innovation (Douma and Palodichuk, 2012). The regulators must therefore recognize and address the uncertainty about the development and deployment of AVs. However, the limits and scope of the regulatory bodies to handle comprehensive social implications in a timely manner remain a concern (Taeihagh and Lim 2018). The following areas are taken for research:

Criminal Law & Enforcement – Considerable analysis has been carried out on civil liability issues in comparison with criminal law and enforcement in AVs (Glancy 2015). The criminal laws should be reconsidered to reflect the risk profile of AVs. AVs can also lead to the creation of new crimes and the misuse of AVs in crimes is another area in which new types of crimes can arise.

Forensic Investigations – To understand what happened in criminal cases that involve AVs, it would be necessary to investigate the systems and other components to provide a sound legal reason for prosecution (Parkinson et al. 2017).

Cybersecurity Laws & Regulations – It is important to consider all possible cybersecurity attacks in the AV systems and protocols at the design stage. Although computer technologies are being used to defend these attacks, appropriate standards and regulations should also be developed to reduce such attacks (He, Meng, and Qu 2017).

Intelligent Transportation Systems (ITS)

ITS cover a wide range of fields to provide safer, efficient and sustainable transport-related services. ITS aims to reduce time, money, and energy costs and improve road congestion and infrastructure management (Friesen and McLeod 2015). ITS would be necessary despite the intrinsic intelligence in AVs since AVs require enormous computing and storage requirements to be fully aware of all conditions in a city and this might not utterly represent a real end-to-end solution for an effective ITS (Turner and Uludag 2016). Although ITS research has started significantly over a decade ago, open research challenges still exist for its success (Hamida, Noura, and Znaidi 2015). The following sub-areas have been identified for research:

Privacy – If the vehicles constantly transmit information to other vehicles and to a control infrastructure, there are high chances to easily track the log details of the vehicles (Simic 2013). The profoundly connected nature of ITS could conflict with the fundamental privacy requirements of passengers (Elbanhawi, Simic, and Jazar 2015). Consequently, the flow, obscurity and storage of this sensitive data are expected to be cautiously administered.

Traffic Congestion – Research studies have shown that congestion alone in transportation systems consumes immense resources (Turner and Uludag 2016). Various researchers differ in their views on the impact of AVs on congestion. Few scholars anticipate reduced traffic delays and congestion, higher transport system reliability and increased vehicle throughput. Few others envision that AVs could have a negative impact on traffic congestion by increasing vehicle-kilometer-traveled and inducing additional demand which could add traffic density and other additional burdens to an already congested network. The overall impact of the AV on congestion has therefore not yet been investigated (Bagloee et al. 2016).

Big Data – "Connectivity" and "Big Data" are believed to be two additional elements for the AV's success. Connectivity requires huge datasets, "Big Data" from a wide range of sources and one of the biggest challenges anticipated is the processing and analysis of Big Data to ensure Vehicle-to-Vehicle and Vehicle-to-Infrastructure connectivity (Bagloee et al. 2016).

Vehicular Ad-Hoc Network (VANET) – VANETs are ad hoc networks used for communication among and between vehicles and roadside units which has the potential to reduce congestion and traffic safety & management. Security Challenges in VANETs are the lack of central points, mobility, wireless links,

cooperativeness, and lack of a clear line of defense. Due to these characteristics, conventional security approaches cannot be directly applied to VANETs (Sakiz and Sen 2017). Researchers have demonstrated how Denial of Service can be performed against VANETs to disrupt the infrastructure. VANET's safety and security aspects are an overlooked area in AVs and it is important to explore them because compromising these control protocols could lead to incorrect decisions that threaten AVs' stability and safety (Amoozadeh, 2015) (Parkinson et al. 2017).

Predictive Measures

AV's decision-making system plays a crucial role in AVs in predicting surrounding vehicles' driving behaviors to provide safe and reasonable abstract driving measures (Geng et al. 2017). Decision-making is difficult because of vulnerability on the constant condition of close-by vehicles and, specifically, because of uncertainty over their movements (Galceran et al. 2017). The following areas are taken for research:

Urban Scenarios – AV's decision-making system needs to predict accurately the future driving behavior which is quite challenging especially in urban roadways. Most driving behavior prediction models work for one specific scenario and cannot be adapted to different scenarios. However, AVs drive through dynamically changing urban environments in which a diversity of scenarios appear over time (Carvalho et al. 2014) and multiple scenario-specific adaptation models should be designed according to the scenario characteristics (Geng et al. 2017).

System Uncertainties – One of the main challenges is to systematically account for the uncertainties due to the presence of other static or moving objects (e.g. vehicles, bicycles, pedestrians). Approaches that do not account for the system's uncertainties can lead to unsafe results (*risk*) and robust control approaches that deal with worst-case disturbances can be excessively *conservative* and expensive. It is still not possible to interpret accurately the traffic scenarios without increasing the computation complexity (Geng et al. 2017). Hence, it is necessary to introduce prediction models to deal with the uncertainties of the system as a trade-off between risk and conservativeness (Carvalho et al. 2014).

Insurance – AVs bring about "evolution" which means that there will a paradigm shift in the definition of "driver" (McChristian and Corbett 2016). This transition will bring about a considerable change in how the dangers associated with AV-related accidents are protected (Crane, Logue, and Pilz 2016). Hence, the traditional auto-insurance models will need to gradually evolve since the existing driver-centric models appear to be inappropriate (Glancy 2015). AVs might bring uncertain liability risks, cyber risks, etc., and hence there is a need for AVs to have a comprehensive risk insurance policy.

Cyber-Attacks

Cyber-attack aims to disrupt, damage or destroy any digital system and currently highly sophisticated and complex attacks have continued to increase (Hansman and Hunt 2005). Increased vehicle autonomy and connectivity often exacerbate the risk of cybersecurity attacks (Parkinson et al. 2017).

Large-scale hacking – Criminal and terrorist attacks on AVs are particularly detrimental and a large-scale attack on vehicles on roads, for example, could cause transportation chaos across a large region. The greater challenge of system-wide hacking, terrorist-related hacking or other prevalent electronic disabling of vehicles is unknown (Kennedy 2016).

Cyber-attack detection – The degree of human involvement in cyber aspects is a less explored area. There are many research articles on attacking and compromising vehicle safety, but there is no literature on how the driverless system warns about detecting a potential cyber-attack (Parkinson et al. 2017).

Phishing & Ransomware attacks – When connected to the AV, the user's device can be used as an attacking mechanism to mount attacks on the AVs via phishing attacks (pretending to be a trusted source for getting sensitive information or compromising the system). It is anticipated that phishing and ransomware (disabling the system or vehicle function until ransom is paid) attacks could take control of the vehicle and potentially create damages to the user. However, there is a lack of research detailing how these attacks could be carried out and how they could be mitigated (Parkinson et al. 2017).

Anticipation of Range of threats – The attack surface for AVs will rapidly broaden as more advanced services and communications systems are incorporated into vehicles. Today, many wireless communication technologies exist and the connectivity between the vehicles has increased the potential points of attack (Carsten et al. 2015). This clearly indicates that there will be a wide range of threat vectors available to an attacker and possibly lead to unknown consequences and significant threats to automations systems (Koscher et al. 2010).

In-Vehicular Network

Controller Area Network (CAN) is a dominant in-vehicle communication network protocol that connects multiple ECUs (Electronic control units). CAN's enormous role in interconnectivity and functionality makes it an irreplaceable part at present. Therefore, the functionality and safety of AVs rely on the safe and secured communication network between ECUs (Haddrell 2016).

CAN's broadcast nature, lack of {authentication, integrity, confidentiality, network segmentation and data encryption} and vulnerability to Denial of Service attack are identified as the current weaknesses of CAN (Buttigieg, Farrugia, and Meli 2017) (Dariz et al. 2017). Simple methods employed in CAN to protect the integrity of the message are widely known to be inadequate

(Zhang, Antunes, and Aggarwal 2014). Potential CAN vulnerabilities against cyber-attacks are therefore unacceptable and could lead to cybersecurity threats (Carsten et al. 2015).

Lack of Authentication – CAN is not equipped to identify the source of messages and is unable to find out whether the messages are legitimate or originate from the legitimate components. This means that any compromised component can easily control all the other components connected within the CAN network (Buttigieg, Farrugia, and Meli 2017).

Potential entry points of attacks – To compete in the market, many companies offer their customers highly sophisticated and value-added services. Many electronic equipment, communication features and third-party applications are introduced and integrated into the system to support these growing functionalities. These trends increase the range of attacks and an attacker can gain access to the vehicle network. Hence, it is essential that a safe environment is provided against malicious attacks (Buttigieg, Farrugia, and Meli 2017) (Wang, Lu, and Qu 2018)

Vulnerabilities of Electronic Control Units (ECU) – Since the CAN lacks enough security and protection, many security-critical ECUs are exposed to attacks. ECUs weak access control allows to be reprogrammed to update them with malicious code. Threats to cybersecurity on an ECU could possibly manipulate the operations of other components (Koscher et al. 2010). Attacking single or multiple ECUs to (1) exploit safety critical operations such as braking, speeding, lighting control systems, etc., (2) send unauthorized communication messages or altering valid messages, (3) flood the bus to create traffic problem could have a major impact or even a fatal failure (Dariz et al. 2017) (Wang, Lu, and Qu 2018).

Attacks on Sensors & Navigation systems – AVs rely on sensing technology and data fusion software to sense their environment and make the right driving decisions. Attacks on sensors, cameras and navigation systems could lead to false data display, malfunctions, damage to vehicle control systems and the potential consequences could be life-threatening for one vehicle or for many vehicles connected to the network (Yan, Xu, and Liu 2016). Several potential attacks are demonstrated by many white-hat hackers on these sensors (Haddrell 2016). However, the extent to which sensors and navigation systems could be compromised and their impact on the function of a vehicle are unclear (Parkinson et al. 2017).

Personal Data Protection – Hackers gained access to personal information of seven million drivers and 57 million Uber's global users. Uber reported theft of data such as names, e-mail addresses, phone numbers, driving license number, etc. (Eric Newcomer 2017). Which type of personal information will be generated and stored in AV systems is still unclear, but possible steps should be taken to protect the privacy of individuals. The location and movement of the vehicle could provide valuable data for targeted theft, advertising purposes, understand behavioral habits and so on (Parkinson et al. 2017).

Trust

Trust is considered critical in adopting and accepting the vehicle automation and earning this trust becomes even more crucial for AVs which has an increasing complexity of automation and vulnerability of the users (Wortham and Theodorou 2017). Trust is the most vital part for humans and robots to work together as a team (Hancock et al. 2011). There are many psychological barriers such as {ethical dilemmas, overreactions to accidents by AVs, overreliance on the AV technology, lack of situational awareness and transparency in predicting AVs behavior} to trust which stand in the way of achieving the potential benefits of AVs (Shariff, Bonnefon, and Rahwan 2017) (Petersen et al. 2017).

Predictability & Comfort – To generate trust, it is important to ensure that people can comfortably predict the driving behavior. AVs decision-making processes are technologically opaque and people may have different assumptions about the extent and capabilities of AVs. Improved education in line with the actual abilities might help to overcome either underestimating or overestimating AVs (Anderson, Kalra, and Wachs 2009). In addition, AVs will need to communicate not just with their occupants, but with pedestrians, drivers and the other road stakeholders (Shariff, Bonnefon, and Rahwan 2017). How AVs interact with manually driven vehicles and vice versa, in "mixed-traffic" situations stay unclear (Cavoli et al. 2017). Therefore, it is critical to investigate what amount and type of information should be communicated to people to foster predictability and comfort in order to generate trust (Shariff, Bonnefon, and Rahwan 2017).

Trust among the entities of ITS – ITS relies on data gathered (by periodic information shared by users) to reduce congestion, make transport safer and efficient. The verification of data aggregation is essential to build trust among ITS entities (Gosman, Dobre, and Pop 2017). The aggregation of data poses significant security risks in ITS and in the absence of protection mechanisms, most of these applications can jeopardize the privacy of participants and end users (Christin 2016). Therefore, a secure, trustworthy, and decentralized architecture should be developed to build a healthier and safer ITS ecosystem and maintain its overall stability, productivity, and efficiency (Yuan and Wang 2016).

Privacy – According to FTC Report on the Internet of Things (IOT) 2015, the technological advancement has surpassed the rules and regulations in cybersecurity and privacy aspects, thereby reducing trust in IOT devices. If AVs follow the same direction, public's trust could be damaged by a major privacy invasion. Some ITS technologies use the location and movement data of the vehicle posing serious privacy threats. Therefore, it is important to establish a high level of trust (Lederman, Taylor, and Garrett 2016).

Human-machine interface (HMI) – HMI acts as the connectivity point between humans and driverless system and for a safe system, optimal design of the HMI is necessary to promote trust. It is essential to keep the vehicle occupants 'in-the-loop' (awareness about the status of vehicles and road traffic situation). This is important

to signal a safer re-engagement during emergencies (Cunningham and Regan 2015).

Trust on V2X Communications – By 2025, each new vehicle is expected to be connected in several ways. ITS will leverage various vehicular communications such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P), and vehicle-to-anything (V2X) to deliver transport-related services. Different companies offer different equipment, systems and technologies and it is therefore vital to standardize ITS to ensure interoperable V2X communications between them irrespective of their brands and models thereby improving the trust on these technologies (Hamida, Noura, and Znaidi 2015).

Research Methodology

Review of academic articles helped to identify the research gap and to determine seven independent variables and its sub-variables. The following framework illustrates the relationship between cyber threats and independent variables:

Data Collection

Primary research was conducted by expert interview and online survey questionnaire. The survey contained 34 questions based on variables/sub-variables (Figure 2) and 4 questions on participant's demographic details. Responses for all questions were measured on a five-point Likert scale.

Profile of Respondents

Pilot-testing was conducted with a sample size of 30 respondents working in automotive industries and AV start-ups. Expert interview was also conducted to gather additional input and after Pre-testing, the final online questionnaire was sent to all the stakeholders of automotive industry. The online questionnaire was sent to Autonomous Vehicle Communities, Automakers and others with driving experience or domain knowledge through social media (LinkedIn, Facebook and WhatsApp). Survey link was distributed to about 650 participants, out of which 203 attended the survey (34% response rate).

Data Analysis

Partial Least Squares path modeling is preferred for research studies for its flexible modeling and identifying key drivers (Hair, Ringle, and Sarstedt 2011). The data analysis was carried out using ADANCO 2.0.1 to develop and evaluate the structural model and the causal relationships between the variables.

Table 1. Overall reliability of variables.

Variables	R^2	Jöreskog's rho (ρc)	Cronbach's alpha (α)
Cyber Threats on AVs	0.436	0.8835	0.8475
Socio-Cultural		0.7886	0.6061
Regulations		0.7957	0.6167
ITS		0.8201	0.708
Predictive Measures		0.8046	0.6352
Cyber attacks		0.8106	0.691
In-vehicular Network		0.8385	0.7575
Trust		0.8454	0.7712

Reliability

The two variable reliability measurements used in this study are (1) Cronbach's alpha (α) and (2) Jöreskog's rho (ρc). Cronbach's alpha coefficient should be between >0.6 and <1 to obtain an acceptable level of reliability (Pallant. 2007). Jöreskog's Rho evaluates "composite reliability" to appreciate the integrity and homogeneity of the model (Werts et al. 1978). All variables have produced acceptable reliability measurements.

Validity

(a) *Convergent Validity*

As (Carlson and Herdman 2012) mentioned, convergent validity evaluates the degree of correspondence between two measures of variables and the cutoff value ≥0.5 is acceptable (Henseler and Dijkstra 2015) (Hair, Ringle, and Sarstedt 2011).

(b) *Discriminant Validity*

Discriminant validity ensures that the constructs that differ from each other are proven to be different (Henseler and Dijkstra 2015). The AVE measure of other variables should be lesser than the square root of AVE obtained from a particular variable table 2. This Fornell-Larcker method is used for evaluating the degree of distinction between the variables (Carless 2004).

Table 2. Average variance extracted (AVE) for each construct.

Variable	Average variance extracted
Cyber Threats on AVs	0.5207
Socio-Cultural	0.5577
Regulations	0.5680
ITS	0.5331
Predictive Measures	0.5791
Cyber attacks	0.5181
In-vehicular Network	0.5158
Trust	0.5232

Table 3. Discriminant validity for each variable.

Construct	Cyber threats on AVs	Socio-cultural	Regulations	Intelligent transportation systems	Predictive measures	Cyber attacks	In-vehicular network	Trust
Cyber Threats on AVs	0.5207							
Socio-Cultural	0.2346	0.5577						
Regulations	0.2006	0.1833	0.568					
Intelligent Transportation Systems	0.2615	0.2203	0.3745	0.5331				
Predictive Measures	0.2053	0.2256	0.0955	0.1847	0.5791			
Cyber attacks	0.1995	0.0976	0.0839	0.1926	0.2597	0.5181		
In-vehicular Network	0.1624	0.1582	0.0951	0.1444	0.3165	0.3731	0.5158	
Trust	0.3094	0.3053	0.1693	0.2073	0.323	0.3174	0.4417	0.5232

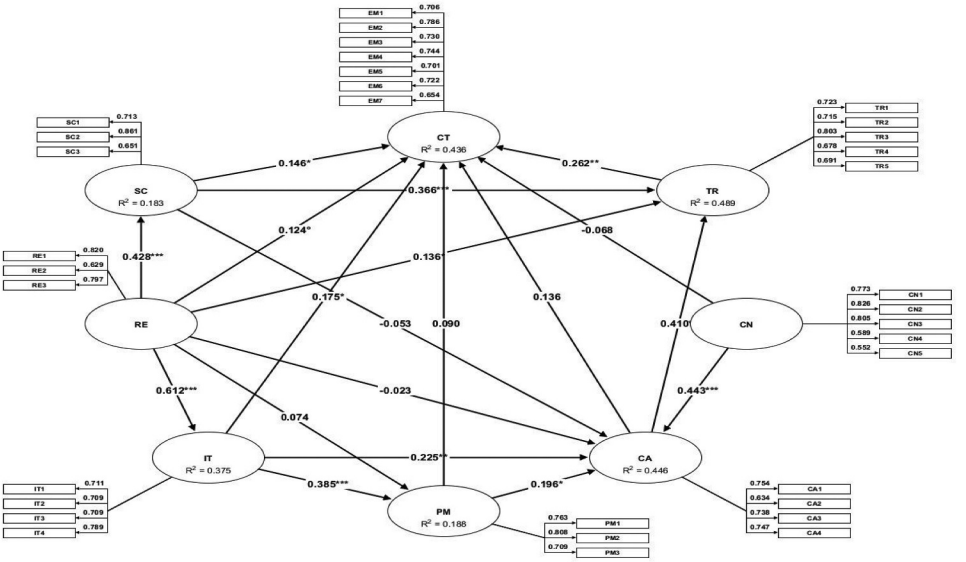


Figure 4. Graphical representation of the model with path coefficients.

(Squared correlations; AVE on the diagonal)

(c) *Indicator Multicollinearity*

Multicollinearity exists when two indicators are correlated to each other providing unnecessary information. If the cutoff value (which is calculated by measuring the variance inflation factor) exceeds 5 table 4, then the indicator is not a significant parameter (Hair, Ringle, and Sarstedt 2011).

Path Analysis

Path analysis or causal modeling depicts the independent variables and dependent variable graphically along with the strength of each path.

Hypotheses Testing

To understand the assumed relationships, the t-values and the *p*-values from the total effects inference table are used to evaluate the impact between variables. To evaluate the parameters of the unknown population, bootstrapping is the simple and appropriate method used in statistics (Efron 1987).

Table 4. Indicator multicollinearity.

Indicator	Cyber threats on AVs	Socio-cultural	Regulations	Intelligent transportation systems	Predictive measures	Cyber attacks	In-vehicular network	Trust
SC1		1.1967						
SC2		1.3272						
SC3		1.1864						
RE1			1.32					
RE2			1.1274					
RE3			1.34					
IT1				1.3638				
IT2				1.3112				
IT3				1.2521				
IT4				1.463				
PM1					1.349			
PM2					1.373			
PM3					1.1463			
CA1						1.2439		
CA2						1.1686		
CA3						1.5693		
CA4						1.6014		
CN1							1.5842	
CN2							2.1656	
CN3							1.8217	
CN4							1.1721	
CN5							1.2486	
TR1								1.4834
TR2								1.431
TR3								1.6965
TR4								1.4183
TR5								1.4087
EM1	1.88							
EM2	2.1127							
EM3	1.8758							
EM4	1.7145							
EM5	1.6533							
EM6	1.6767							
EM7	1.5058							

The above table shows that there is no multicollinearity.

Findings

The path coefficient of 16 hypotheses is highly significant, two hypotheses *H8* and *H15* have a significant impact and the hypotheses *H14* and *H16* have a moderate impact. Hence, all these hypotheses are accepted. However, *H2* and *H19* have shown that they have no effect and have therefore been rejected. The cutoff values suggested by (Bullmore et al. 2000) were taken to measure the strength of the path coefficient for each sub-variable; 0.5–0.8 means

Table 5. Levels of significance to evaluate the significance of variable's relationship.

Significance	t-value	Confidence interval
$p < .1$	≥ 1.65	90%
$p < .05$	≥ 1.96	95%
$p < .01$	≥ 2.59	99%

Table 6. Hypotheses testing (total effects inferences).

			Standard bootstrap results					Percentile bootstrap quantiles				
Hypotheses	Effect	Original coefficient	Mean value	Standard error	t-value	p-value (2-sided)	p-value (1-sided)	0.50%	2.50%	97.50%	99.50%	Supported?
H1	SC -> CT	0.2292	0.2278	0.0748	3.063	0.0022	0.0011	0.0531	0.0894	0.3694	0.4139	Yes
H2	SC -> CA	−0.0527	−0.053	0.0788	−0.668	0.5043	0.2521	−0.2248	−0.197	0.1074	0.1525	No
H3	SC -> TR	0.3448	0.3428	0.0575	6.0004	0	0	0.1893	0.2253	0.4553	0.4918	Yes
H4	RE -> CT	0.4355	0.44	0.0733	5.9404	0	0	0.2341	0.2931	0.5832	0.6152	Yes
H5	RE -> SC	0.4282	0.4387	0.0775	5.5217	0	0	0.2361	0.2747	0.5779	0.6253	Yes
H6	RE -> IT	0.612	0.6163	0.0532	11.4946	0	0	0.4558	0.5011	0.7126	0.7413	Yes
H7	RE -> PM	0.309	0.3167	0.081	3.8171	0.0001	0.0001	0.1102	0.1714	0.48	0.5269	No
H8	RE -> CA	0.1529	0.1582	0.0762	2.0061	0.0451	0.0226	−0.0515	0.0049	0.3068	0.3522	No
H9	RE -> TR	0.3554	0.3605	0.0735	4.8377	0	0	0.1745	0.2139	0.5063	0.5677	Yes
H10	IT -> CT	0.2826	0.2791	0.0875	3.2309	0.0013	0.0006	0.0657	0.1051	0.4585	0.5117	Yes
H11	IT -> PM	0.3848	0.3771	0.1082	3.5568	0.0004	0.0002	0.0988	0.1596	0.5863	0.6378	Yes
H12	IT -> CA	0.3002	0.2933	0.0914	3.2842	0.0011	0.0005	0.0304	0.1144	0.4776	0.5295	Yes
H13	IT -> TR	0.1229	0.1217	0.0399	3.0822	0.0021	0.0011	0.0133	0.0462	0.2009	0.2279	
H14	PM -> CT	0.1376	0.1359	0.0793	1.7358	0.0829	0.0415	−0.0538	−0.0134	0.2955	0.3418	No
H15	PM -> CA	0.1956	0.1883	0.0928	2.1069	0.0354	0.0177	−0.0489	−0.0037	0.3768	0.4242	Yes
H16	PM -> TR	0.0801	0.0789	0.0412	1.9437	0.0522	0.0261	−0.0212	−0.0018	0.1694	0.1949	
H17	CA -> CT	0.2436	0.2512	0.0909	2.6809	0.0075	0.0037	0.0334	0.0802	0.436	0.4834	No
H18	CA -> TR	0.4096	0.4154	0.0506	8.0959	0	0	0.2724	0.3107	0.5111	0.5445	Yes
H19	CN -> CT	0.0402	0.0454	0.0747	0.5382	0.5906	0.2953	−0.1566	−0.1038	0.1867	0.2204	No
H20	CN -> CA	0.4433	0.4489	0.0805	5.5081	0	0	0.2358	0.2896	0.6009	0.6414	Yes
H21	CN -> TR	0.1816	0.1876	0.0454	3.9995	0.0001	0	0.0828	0.1053	0.2837	0.3145	
H22	TR -> CT	0.262	0.2636	0.0985	2.6591	0.008	0.004	0.0099	0.0682	0.4627	0.5061	Yes

Note: SC (Socio-cultural), CA (Cyber Attacks), TR (Trust), CT (Cyber Threats on AVs), RE (Regulations), IT (Intelligent Transportation systems, PM (Predictive Measures), CN (In-vehicular Network)

a moderate effect while >0.8 indicates a strong effect on the independent variable. The findings of 22 hypotheses are explained below:

Socio-Cultural

Figure 4 shows that vehicle occupants want an information system in AVs that does not provide excessive information and increase their mental workload, which would otherwise have a negative impact on safety. *H1* (t-value 3.063; $p < .01$) is accepted indicating that the impact of socio-cultural factors on cyber threats is highly significant. Similarly, *H3* (t-value 6.0004; $p < .01$) is accepted which signifies a highly significant effect of socio-cultural factors on Trust. There would be an increased trust if the AVs provide safe and efficient take-over, clarity in remedial procedures during accidents and adequate vehicle information. However, *H2* (t-value −0.668) is rejected showing that there is no impact of socio-cultural factors through three sub-variables on cyber-attacks. Overall, we found a strong correlation between the "workload of the driverless system" with cyber-attacks and cyber threats to AVs. This relationship has not been mentioned in prior studies.

Regulations

Figure 4 shows that the criminal law and enforcement issues relating to AVs have a strong impact on the regulations. Forensic investigations and cybersecurity laws affect the regulations moderately.

All the above six hypotheses *H4* – *H9* are accepted based on the t-value. This signifies the impact of regulations on several aspects. This is in line with the earlier studies that argued that Regulatory rather than technological obstacles could become a practical barrier to AV technology implementation (Brodsky 2016). Regulations have a highly significant effect on cyber threats, cyber-attacks, socio-

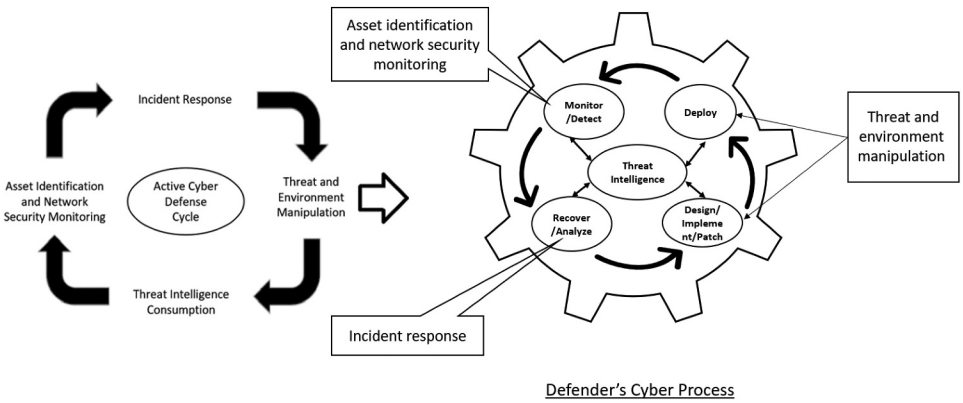


Figure 5. Active Cyber Defense Cycle correlated with Defender's cyber process.

cultural factors, intelligent transportation systems, predictive measures and trust. It is clear from these results that criminal law and enforcement issues (if not addressed) have a huge impact on cyber threats. In addition, regulatory intervention in the personal data protection and privacy requirements of passengers, safety and security of the vehicle network, insurance risks, standardizing AV behavior for predictability, educating the public about the actual capabilities of AVs, and bringing trust among the entities of ITS are necessary. Furthermore, product liability framework for remedial procedures should be in place to avoid any liability issues which might impede the success of AVs. These findings are in line with the earlier studies by (Glancy 2015) (Surden and Williams 2016) (Bloom et al. 2017).

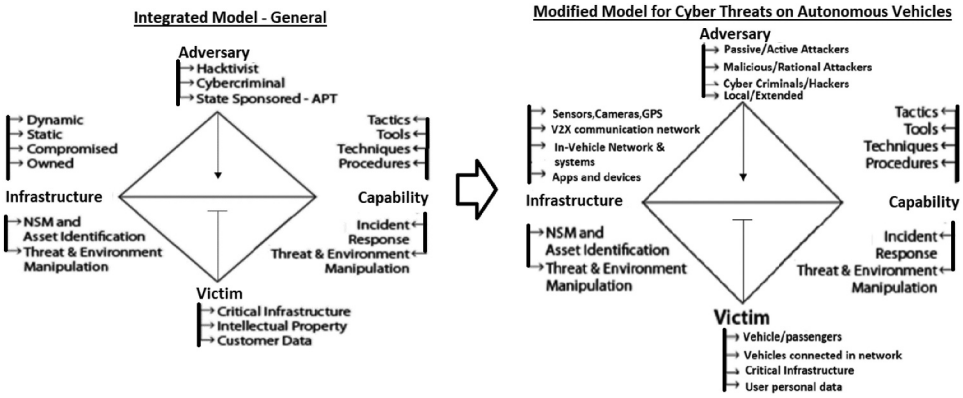


Figure 6. Integrated Model – General & Modified; NSM – Network security monitoring, APT – Advanced persistent threat.

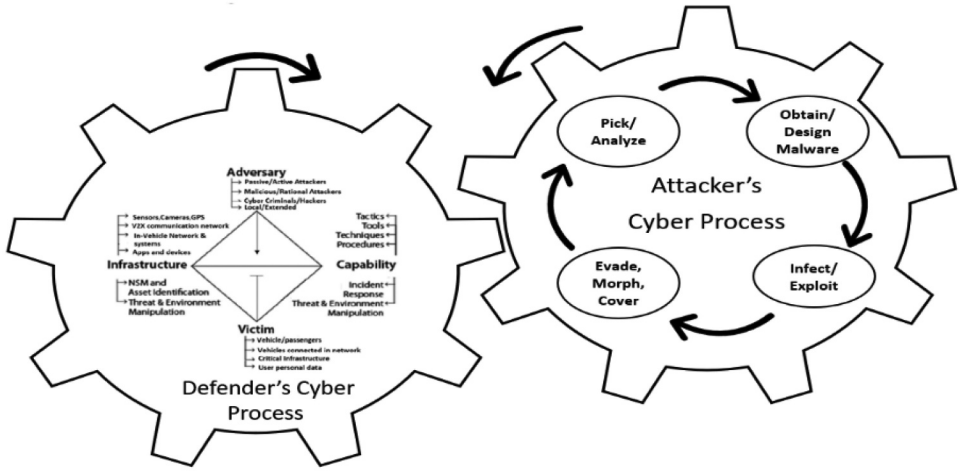


Figure 7. Modified Cyber cycle Theory.

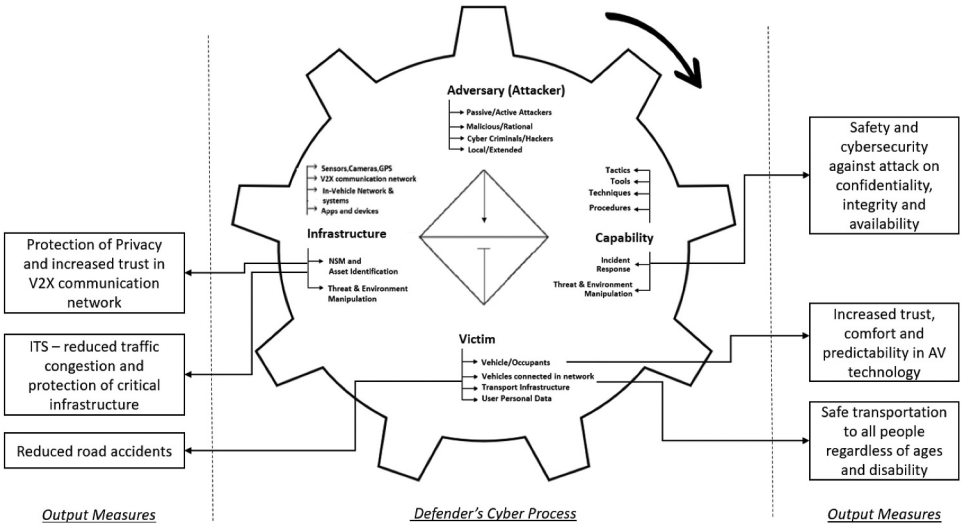


Figure 8. Modified Defender's cyber process with Research output measures.

Intelligent Transportation Systems

Figure 4 shows that all the sub-variables of ITS have a moderate impact on the ITS.

All the above four *H10 – H13* assumptions are accepted based on the t-value. This means that ITS has a high impact on several aspects. ITS has a very significant impact on cyber threats, cyber-attacks, predictive measures and trust through its sub-variables such as privacy, traffic congestion, Big data and VANET. Trust in ITS and cybersecurity depends on how parameters such as (1) the safety and security of VANET protocols against attacks, (2) processing and analysis of Big Data to ensure interconnectivity among and between vehicles and control systems, (3) AVs impact on traffic congestion, and (4) flow, obscurity and storage of personal and vehicle information are handled in ITS ecosystem. This is in accordance with the findings of the previous research studies (Elbanhawi, Simic, and Jazar 2015) (Bagloee et al. 2016) (Amoozadeh, 2015) (Sakiz and Sen 2017).

Predictive Measures

Figure 4 shows that the AVs driving behavior accounting for system uncertainties have a strong impact on the predictive measures. *H14* (t-value 1.7358; $p < .1$) *and H16* (t-value 1.9437; $p < .1$) show that predictive measures have a moderate impact on cyber threats and trust through designing prediction models for dynamic urban scenarios, comprehensive insurance risks policy and system uncertainties. H*15* (t-value 2.1069; $p < .05$) tested the effects of predictive measures on cyber-attacks and the results show that the effects are significant. It is determined from this study that predicting driving behavior with accurate perception and interpretation to

face the system uncertainties (dynamic traffic scenarios and surrounding entities) that requires a trade-off between safety risks and expensive computational complexity has a significant impact on possibility of cyber-attacks. This substantial correlation is not addressed in any of the previous research studies.

Cyber Attacks

Figure 4 shows that all four sub-variables affect cyber-attacks moderately. *H17* (t-value 2.6809; $p < .01$) *and H18* (t-value 8.0959; $p < .01$) are accepted, showing that the effects of cyber-attacks on cyber threats and trust are extremely significant and intuitive. Cyber-attacks through its sub-variables, such as (1) large-scale cyber risk of hacking on vehicles, (2) designing driverless systems to alert against attacks, (3) phishing and ransomware attacks on vehicles and (4) anticipating a wide range of threat vectors, strongly influence the possibility of cyber threats against AVs. These findings are in line with the earlier studies (Kennedy 2016) (Parkinson et al. 2017).

In-Vehicular Network

Figure 4 shows that the potential attack points on AVs and vulnerabilities of ECU have a strong impact on the in-vehicle network. All the other three variables affect the in-vehicle network moderately. *H19* (t-value 0.5382) is rejected indicating that the in-vehicle network does not have an impact on cyber threats through its sub-variables. However, *H20* (t-value 5.5081; $p < .01$) shows that the in-vehicle network strongly influences cyber-attacks, which explains that they also influence cyber threats indirectly. Parameters such as ECU weaknesses, possible attack surfaces of AVs adversely affecting the in-vehicle network, attacks on sensors and navigation systems and the personal data protection by influencing in-vehicular network impact the cyber-attacks. *H22* (t-value 3.9995; $p < .01$) is also accepted signifying the highly important correlation between in-vehicle network and trust on AVs.

From this study, it is examined that vulnerabilities of ECU and possible attack entry points by strongly impacting in-vehicle network influence cyber threats highly significantly. These are in line with the earlier studies (Parkinson et al. 2017) (Koscher et al. 2010). In addition, the impact of in-vehicle network on trust is highly significant. This shows that ECU vulnerabilities, CAN weaknesses and wide attack entry points if not addressed properly, this might pose a great security threat thereby diminishing trust on AVs. This correlation of in-vehicular network vulnerabilities with trust is not touched upon in earlier studies.

Trust

Figure 4 shows that the privacy issues in AVs have a strong impact on the trust factor. *H22* (t-value 2.6591; $p < .01$) is accepted which signifies that effect of trust on cyber threats on AVs is highly significant. Trust on vehicular communication network, mutual trust among the ITS entities, predictability and comfort on AVs, privacy issues and human-machine interface strongly impact the cyber threats on AVs. Privacy breach poses a strong threat to cybersecurity and seriously damages public trust hampering the adoption of AV technology. Hence, it is important to establish a high level of trust by protecting information against misuse or disclosure through greater transparency in the technologies and regulations governing the data used (Lederman, Taylor, and Garrett 2016).

Contributions

The results obtained from this study indicate that most of the factors have a positive influence on the cyber threats. Correlation of in-vehicular network vulnerabilities with trust and the correlation between the "workload of the driverless system" with cyber-attacks and cyber threats to AVs are two relations which have not been touched upon in previous studies.

The following are the research answers to the questions mentioned in Section 1.5:

(1) Socio-cultural factors such as re-engagement, workload of driverless system and liability issues have a highly significant influence on cyber threats on autonomous vehicles.
(2) Impact of regulatory matters on criminal law enforcement, forensic investigations and cybersecurity laws on cyber threats on autonomous vehicles is highly significant.
(3) Privacy, Vehicular Ad-hoc network, Big data and Traffic congestion in Intelligent Transportation Systems show a very significant influence on cyber threats on autonomous vehicles.
(4) The influence of dynamic urban traffic scenarios, system uncertainties and insurance risks on cyber threats on autonomous vehicles is moderate.
(5) Large-scale hacking, cyber-attack detection, phishing, ransomware attacks and anticipation of range of threats influences cyber threats on autonomous vehicles highly significantly.
(6) Weaknesses of In-vehicular Network such as lack of authentication, potential entry points of attacks, vulnerabilities of Electronic control units, attacks on sensors & navigation systems and personal data protection positively impacts cyber-attacks but does not show any impact on cyber threats on autonomous vehicles.

(7) The impact of predictability, comfort, trust among the entities of Intelligent transportation systems, privacy, Human-machine interface (HMI), and Trust on V2X Communications on cyber threats on autonomous vehicles is highly significant.
(8) The Active Cyber Defense Cycle (Lee, 2015) is a defensive cyber strategy executed on one's own network and systems Figure 5. It consists of four phases that are continuous, concurrent and interrelated and the phase "Threat intelligence consumption" is a key component that adds value to other three phases. This phase is added to the defender's cyber process of Cyber cycle; in addition, all the other 3 phases are corelated with the four processes in the defender's cyber process of Cyber cycle as below:

Diamond Model of Intrusion Analysis (Caltagirone 2015) provides a flexible model for collecting information on the cyber-threat intelligence of an attacker. It is based on four core features: the adversary, capability, infrastructure and victim. The researcher (Mandt 2017) has integrated this Diamond Model with the Active Cyber Defense Cycle to provide a useful model for maintaining situational awareness of both the activities of an attackers and the cyber-defense activities and capabilities of protectors. The integrated model is customized to show the cyber threats operating environment of AVs in the Figure 6.

Improving the Cyber cycle with the above modified model of two theories produces the following:

It is examined that cyber cycle theory modified with integrated model of Diamond Intrusion theory and Active Cyber Defense Cycle can be applied on cyber threats on AVs Figure 7. This improved theory gives defenders a more proactive cyber-threat intelligence analysis of attackers with the defender's cyber process. The following diagram shows the output measures of this research of the Defender's cyber process of the modified Cyber Cycle: Figure 8

In addition, according to the study results, strict, proactive and adequate regulations on criminal law and enforcement (which strongly influences cyber threats) pertaining to AVs might deter the attackers to perform attacks and slow down the cyber cycle. Strong policies should be in place to punish the cyber criminals.

Implications for the Automotive Industry

Cybersecurity, a biggest threat to AVs must be given critical importance right from the "Design" stage and embedded in the culture of development and maintenance. Cyber threats if less addressed can have severe consequences for the operations of companies (functions, reputation and assets). In addition, potential range of threat vectors ought to be identified for creating user acceptance and adoption of AVs. People may have

different expectations about the extent and capabilities of autonomous vehicles which may not align with its actual abilities. They may either underestimate AVs leading to deadlock and safety problems or inefficiencies (by acting unduly cautious with AVs) or overestimate and expect AVs to operate with near perfect accuracy. Hence, educating public on the actual capabilities of AVs is crucial to avoid over-reliance or overreactions for promoting user acceptance of AVs. This study has shown that protection of privacy is a strong influencing factor on trust and hence focus on privacy is critical. Otherwise, there would be difficulty in getting information from traffic participants. Finally, the success of AVs depends on public–private partnerships, governments, researchers, technology companies and automobile manufacturers.

Limitations and Scope for Future Research

This research was conducted to understand several factors that influences cyber threats on AVs and the effect of those factors. Most of the participants who attended the survey were from Asia-pacific. Participation from other regions would have added little more value to this research. Autonomous vehicles studied in this research belong to the first generation of AVs that might give control to humans during certain situations or events. This paper considered the integration of the Diamond Model of Intrusion Analysis and Active Cyber Defense Cycle with the defender's cyber process in the Cyber cycle and the output measures are shown from a conceptual perspective and a further study exercise testing the usefulness of this integration to validate it can bring significant benefits. This research could be further guided on other factors such as socio-economic factors that impact the cyber threats. Future studies can be conducted on cybersecurity in devising and controlling Intelligent transportation systems and control infrastructure.

Conclusion

Few companies have announced that in early 2019, they will release AVs on a commercial scale (Google's Waymo, Volkswagen's self-driving ride-hailing service in Israel [66]). Since AVs are at the crossroads, this research was conducted to find out the significant factors and investigate their impact on "Cyber Threats on Autonomous Vehicles." Several sub-variables for each of those factors have been identified and the significance of those sub-variables are studied. According to the hypotheses results, socio-cultural factors, regulations, intelligent transportation systems, cyber-attacks and trust have a strong significant impact on cyber threats and the in-vehicular network has a strong influence on cyber-attacks. Other results include criminal law and enforcement strongly influencing the regulations,

privacy issues having high significant impact on trust, strong effect of workload of driverless systems on socio-cultural factors and system uncertainties with trade-off between risk and conservativeness strongly influencing predictive measures. In addition, the defender's cyber process in the Cyber cycle theory was unified with the integrated model of Diamond Model of Intrusion Analysis with the Active Cyber Defense Cycle and the research output measures are shown.

ORCID

Nitin Patwa http://orcid.org/0000-0003-4539-0551

References

Adams, M. D., S. D. Hitefield, B. Hoy, M. C. Fowler, and T. C. Clancy. 2013. Application of cybernetics and control theory for a new paradigm in cybersecurity. *arXiv Preprint arXiv* 1311:0257.

Amoozadeh, M., A. Raghuramu, C. N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine* 53 (6):126–32. doi:10.1109/MCOM.2015.7120028.

Anderson, J. M., et al. 2014. Rand corp., autonomous vehicle technology: A guide for policymakers. 18–28. ; Sarwant Singh, The 10 Social and Tech Trends That Could Shape the Next Decade, FORBES (May 12, 2014, 12:54 PM), http://www.forbes.com/sites/sarwant-singh/2014/05/12/the-top-10-mega-trendsof-the-decade/. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf.

Anderson, J. M., N. Kalra, and M. Wachs. 2009. Liability and regulation of autonomous vehicle technologies. RAND Corporation, Berkeley, CA. http://www. rand. org/pubs/external_publications/EP20090427. html.

Bagloee, S. A., M. Tavana, M. Asadi, and T. Oliver. 2016. Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation* 24 (4):284–303. doi:10.1007/s40534-016-0117-3.

Bloom, C., J. Tan, J. Ramjohn, and L. Bauer. July 2017. Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. Symposium on Usable Privacy and Security (SOUPS).

Bonnefon, J.-F., A. Shariff, and I. Rahwan. 2016. The social dilemma of autonomous vehicles. *Science.* 352 (6293):pp. 1573–1574. doi:10.1126/science.aaf2654.

Brodsky, J. S. 2016. Autonomous vehicle regulation: How an uncertain legal landscape may hit the brakes on self-driving cars. *Berkeley Technology Law Journal* 31:851.

Bullmore, E. T., B. Horwitz, G. D. Honey, M. J. Brammer, S. C. R. Williams, and T. Sharma. 2000. How good is good enough in path analysis of fMRI data? *NeuroImage* 11:289–301. doi:10.1006/nimg.2000.0544.

Buttigieg, R., M. Farrugia, and C. Meli. December 2017. Security issues in controller area networks in automobiles. Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2017 18th International Conference, IEEE, 93–98.

Caltagirone, S. 2015. The cost of bad threat intelligence. viewed 6 February 2017. http://www.activeresponse.org/the-cost-of-bad-threat-intelligence/

Carless, S. A. 2004. Discriminant validity. In *Encyclopedia of social science research methods*, 273. doi:10.4135/9781412950589.

Carlson, K. D., and A. O. Herdman. 2012. Understanding the impact of convergent validity on research results. *Organizational Research Methods* 15:17–32. doi:10.1177/1094428110392383.

Carsten, P., T. R. Andel, M. Yampolskiy, J. T. McDonald, and S. Russ. September 2015. A system to recognize intruders in controller area network (CAN). Proceedings of the 3rd International Symposium for ICS & SCADA Cybersecurity Research. BCS Learning & Development Ltd, 111–14.

Carvalho, A., Y. Gao, S. Lefevre, and F. Borrelli. September 2014. Stochastic predictive control of autonomous vehicles in uncertain environments. 12th International Symposium on Advanced Vehicle Control, 712–19.

Cavoli, C., B. Phillips, T. Cohen, and P. Jones. 2017. Social and behavioural questions associated with automated vehicles a literature review. UCL Transport Institute January.

Christin, D. 2016. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software* 116:57–68. doi:10.1016/j.jss.2015.03.067.

Cohen, T., P. Jones, and C. Cavoli. 2017. *Social and behavioural questions associated with automated vehicles*. UCL Transport Institute: London, UK.

Crane, D. A., K. D. Logue, and B. C. Pilz. 2016. A survey of legal issues arising from the deployment of autonomous and connected vehicles. *Michigan Telecommunications and Technology Law Review* 23:191.

Cunningham, M., and M. A. Regan. October 2015. Autonomous vehicles: Human factors issues and future research. Proceedings of the 2015 Australasian Road Safety Conference.

Daly, I. F. D. P. F. S. J., B. Endicott-Popovsky, and J. Wendleberger. 2002. *White paper #2 – Tranforming cybersecurity research: The deming analogy, draft*. University of Washington, Tech. Rep..

Dariz, L., M. Selvatici, M. Ruggeri, G. Costantino, and F. Martinelli. June 2017. Trade-off analysis of safety and security in CAN bus communication. 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2017, Naples, Italy, 226–31.

Douma, F., and S. A. Palodichuk. 2012. Criminal liability issues created by autonomous vehicles, 52. *Santa Clara Law Review* 1157.

Efron, B. 1987. Better bootstrap confidence intervals. *Journal of the American Statistical Association* 82 (397):171–85. doi:10.2307/2289144.

Elbanhawi, M., M. Simic, and R. Jazar. 2015. In the passenger seat: Investigating ride comfort measures in autonomous cars. *IEEE Intelligent Transportation Systems Magazine* 7 (3):4–17. doi:10.1109/MITS.2015.2405571.

Eric Newcomer. November 22, 2017. Uber paid hackers to delete stolen data on 57 million people. https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

Fitch, G., D. Bowman, and R. Llaneras. 2014. Distracted driver performance to multiple alerts in a multiple-conflict scenario. *Human Factors* 56 (8):1497–505. doi:10.1177/0018720814531785.

Fraedrich, E., S. Beiker, and B. Lenz. 2015. Transition pathways to fully automated driving and its implications for the sociotechnical system of automobility. *European Journal of Futures Research* 3 (1):11. doi:10.1007/s40309-015-0067-8.

Friesen, M. R., and R. D. McLeod. 2015. Bluetooth in intelligent transportation systems: A survey. *International Journal of Intelligent Transportation Systems Research* 13 (3):143–53. doi:10.1007/s13177-014-0092-1.

Galceran, E., A. G. Cunningham, R. M. Eustice, and E. Olson. 2017. Multipolicy decision-making for autonomous driving via changepoint-based behavior prediction: Theory and experiment. *Autonomous Robots* 41 (6):1367–82. doi:10.1007/s10514-017-9619-z.

Geels, F. W. 2005 December The dynamics of transitions in socio-technical systems: A multi-level analysis of the transition pathway from horsedrawn carriages to automobiles (1860--1930). *Technology Analysis & Strategic Management* 17(4):445–76. doi: 10.1080/09537320500357319.

Geng, X., H. Liang, B. Yu, P. Zhao, L. He, and R. Huang. 2017. A scenario-adaptive driving behavior prediction approach to urban autonomous driving. *Applied Sciences* 7 (4):426. doi:10.3390/app7040426.

Glancy, D. J. 2015. Autonomous and automated and connected cars-oh my: First generation autonomous cars in the legal ecosystem. *Minnesota Journal of Law, Science & Technology* 16:619.

Gosman, C., C. Dobre, and F. Pop. May 2017. Privacy-preserving data aggregation in intelligent transportation systems. Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium, IEEE, 1059–64.

Griffin, M. L. 2018. Steering (or not) through the social and legal implications of autonomous vehicles. *Journal of Business, Entrepreneurship & the Law* 11:81.

Haddrell, M. 2016. *Towards an autonomous vehicle enabled society: Cyber attacks and countermeasures*.

Hair, J. F., C. M. Ringle, and M. Sarstedt. 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice* 19 (2):139–52. doi:10.2753/MTP1069-6679190202.

Hamida, E. B., H. Noura, and W. Znaidi. 2015. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics* 4 (3):380–423. doi:10.3390/electronics4030380.

Hancock, P. A., D. R. Billings, K. E. Oleson, J. Y. Chen, E. De Visser, and R. Parasuraman. 2011. A meta-analysis of factors influencing the development of human-robot trust (No. ARL-TR-5857). Army research lab aberdeen proving ground md human research and engineering directorate.

Hansman, S., and R. Hunt. 2005. A taxonomy of network and computer attacks. *Computers & Security* 24 (1):31–43. doi:10.1016/j.cose.2004.06.011.

He, Q., X. Meng, and R. Qu. May 2017. Survey on cybersecurity of CAV. Cooperative Positioning and Service (CPGP), 2017 Forum. IEEE, 351–54.

Henseler, J., and T. K. Dijkstra. 2015. *ADANCO 2.0*. Kleve, Germany: Composite Modeling.

Kamhoua, C., A. Martin, D. K. Tosh, K. A. Kwiat, C. Heitzenrater, and S. Sengupta. November 2015. Cyber-threats information sharing in cloud computing: A game theoretic approach. Cybersecurity and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference, IEEE, 382–89.

Keith Naughton Humans Are Slamming into Driverless Cars and Exposing a Key Flaw. December 2015 https://www.bloomberg.com/news/articles/2015-12-18/humans-are-slamming-into-driverless-cars-and-exposing-a-key-flaw

Kennedy, C. 2016. New threats to vehicle safety: How cybersecurity policy will shape the future of autonomous vehicles. *Michigan Telecommunications and Technology Law Review* 23:343.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, … S. Savage. May 2010. Experimental security analysis of a modern automobile. Security and Privacy (SP), 2010 IEEE Symposium. IEEE, 447–62.

Lederman, J., B. D. Taylor, and M. Garrett. 2016. A private matter: The implications of privacy regulations for intelligent transportation systems. *Transportation Planning and Technology* 39 (2):115–35. doi:10.1080/03081060.2015.1127537.

Lee, R. M. 2015a. Active cyber defense cycle. viewed 6 February 2017, http://www.irongeek.com/i.php?page=videos/bsideshuntsville2015/active-cyber-defense-cyclerobert-m-lee

Mandt, E. J. 2017. Integrating cyber-intelligence analysis and active cyber-defence operations. *Journal of Information Warfare* 16 (1):31–48.

McChristian, L., and R. Corbett. 2016. Regulatory issues related to autonomous vehicles. *Journal of Insurance Regulation* 35 (7).

McMorrow, D. November 2010. Science of cybersecurity. Jason, MITRE Corporation, McLean, VA, Tech. Rep..

Pallant., J. 2007. *SPSS Survival Manual*. 3rd ed. Crows West, New South Wales.

Parkinson, S., P. Ward, K. Wilson, and J. Miller. 2017. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems* 18 (11):2898–915. doi:10.1109/TITS.2017.2665968.

Petersen, L., D. Tilbury, X. J. Yang, and L. Robert. 2017. *Effects of augmented situational awareness on driver trust in semi-autonomous vehicle operation*.

Petit, J., and S. E. Shladover. 2015. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems* 16 (2):546–56.

Sakiz, F., and S. Sen. 2017. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks* 61:33–50. doi:10.1016/j.adhoc.2017.03.006.

Shariff, A., J. F. Bonnefon, and I. Rahwan. 2017. Psychological roadblocks to the adoption of self-driving vehicles. *Nature Human Behaviour* 1 (10):694. doi:10.1038/s41562-017-0202-6.

Simic, M. N. October 2013. Vehicular ad hoc networks. Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference (Vol. 2, pp. 613–18). IEEE.

Surden, H., and M. A. Williams. 2016. Technological opacity, predictability, and self-driving cars. *Cardozo Law Review* 38:121.

Taeihagh, A., and H. S. M. Lim. 2018. Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews* 1–26.

Toews, R. August. 25, 2016. The biggest threat facing connected autonomous vehicles is cybersecurity. Techcrunch. https://techcrunch.com/2016/08/25/the-biggest-threatfacing-connected-autonomous-vehicles-is-cybersecurity/.

Turner, S. W., and S. Uludag April, 2016. Intelligent transportation as the key enabler of smart cities. Network Operations and Management Symposium (NOMS), 2016 IEEE/IFIP (pp. 1261–64). IEEE.

Villasenor, J. April 2014. Products liability and driverless cars: issues and guiding principles for legislation. Brookings. https://www.brookings.edu/research/products-liability-and-driverless-cars-issues-and-guiding-principles-for-legislation/

Volkswagen, Intel, and Mobileye will launch a self-driving taxi service in Israel. 2019. https://www.theverge.com/2018/10/29/18039216/volkswagen-intel-mobileye-self-driving-ride-hailing-israel–2019

Wang, Q., Z. Lu, and G. Qu. 2018. An entropy analysis based intrusion detection system for controller area network in vehicles. *arXiv Preprint arXiv* 1808:04046.

Werts, C. E., D. R. Rock, R. L. Linn, and K. G. Joreskog. 1978. A general method of estimating the reliability of a composite. *Educational and Psychological Measurement* 38 (4):933–38. doi:10.1177/001316447803800412.

Wortham, R. H., and A. Theodorou. 2017. Robot transparency, trust and utility. *Connection Science* 29 (3):242–48. doi:10.1080/09540091.2017.1313816.

Wu, C., and Y. Liu. 2007. Queuing network modeling of driver workload and performance. *IEEE Transactions on Intelligent Transportation Systems* 8 (3):528–37. doi:10.1109/TITS.2007.903443.

Yan, C., W. Xu, and J. Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. DEF CON. 24.

Yuan, Y., and F. Y. Wang. November 2016. Towards blockchain-based intelligent transportation systems. Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference (pp. 2663–68). IEEE.

Zeeb, K., A. Buchner, and M. Schrauf. 2015. What determines the take-over time? An integrated model approach of driver take-over after automated driving. *Accident Analysis & Prevention* 78:212–21. doi:10.1016/j.aap.2015.02.023.

Zhang, T., H. Antunes, and S. Aggarwal. 2014. Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things Journal* 1 (1):10–21. doi:10.1109/JIOT.2014.2302386.