THESIS

EVALUATING FACTORS THAT IMPACT SITUATION AWARENESS AND TAKEOVER RESPONSES DURING CYBERATTACKS ON CONNECTED AND AUTOMATED VEHICLES

Submitted by

Somayeh Aliebrahimi

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Fall 2022

Master's Committee:

Advisor: Erika Miller

Thomas Bradley
Ann Batchelor
Benjamin Clegg

ABSTRACT

EVALUATING FACTORS THAT IMPACT SITUATION AWARENESS AND TAKEOVER RESPONSES DURING CYBERATTACKS ON CONNECTED AND AUTOMATED VEHICLES

Autonomous vehicles offer many potential benefits; however, this expansion of cyber-physical systems into transportation also introduces a new potential vulnerability in terms of cybersecurity threats. It is therefore important to understand the role vehicle occupants can play in preventing and responding to cyberattacks. The objectives of this study are to *(1)* evaluate how drivers respond to unexpected cyberattacks on automated vehicles, *(2)* evaluate how cybersecurity knowledge affects situation awareness (SA) during cyberattacks on automated driving, and *(3)* evaluate how the type of cyberattack affects a drivers' response.

A driving simulator study with 20 participants was conducted to measure drivers' performance during unexpected cyberattacks on a SAE Level 2 partially-autonomous vehicle and the infrastructure in the driving environment. The scenarios were developed specifically for use in this study. Each participant experienced four driving scenarios, each scenario with a different cyberattack. Two cyberattacks were directly on the vehicle and two were on the infrastructure. Situation Awareness Global Assessment Technique (SAGAT) was used to measure participants' situation awareness during the drives and at the time of the cyberattacks. Participant takeover responses to the cyberattacks were collected through the driving simulator. Participants

also completed a cybersecurity knowledge survey at the end of the experiment to assess their previous overall cyber awareness and experience with autonomous vehicles.

Most of the participants noticed the cyberattacks, however only about half of the participants chose to take over control of the vehicle during the attacks, and in one attack no one overtook the automation. Results from ANOVAs showed significantly higher SA for participants with greater familiarity with cybersecurity terms and vehicle-to-everything technology. In addition, SA scores were significantly higher for participants who believed security systems (i.e., firewall, encryption) are important and for those who felt protected against cybercrimes. The present results suggest that increased cybersecurity knowledge can cause a high level of situation awareness during automated driving, which can help drivers to control unexpected driving situations due to cybersecurity attacks. Additionally, the results show that drivers are more likely to takeover control of their automated vehicle for cyberattacks that have known adverse outcomes, such as failing to stop at a stop sign or traffic signal or when their vision is obscured.

DEDICATION

Dedicated to my family

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1. Overview

This study aims to evaluate drivers' reaction to cyberattacks on connected and automated vehicles (CAVs). Our research also looks for factors that have impacts on drivers' situation awareness and their responses to cyberattack on automated vehicles. We seek to evaluate people's cybersecurity awareness in general and in CAVs to identify how the level of cybersecurity awareness can help drivers to respond to unexpected cyberattacks.

Many automotive manufacturers and researchers are working with new technologies to secure CAVs from cyber threats, however, it is increasingly difficult to find a solution to prevent all cyberattacks as quantity and varieties of technologies in CAVs continues to grow (Zhang et al., 2019). In addition to cybersecurity technologies in connected systems, it is important to consider the human-in-the-loop framework to evaluate behavior of humans who need to perform security-critical functions in response to cyberattacks (Cranor, 2008). As such, the way that drivers respond to unexpected cyberattacks plays an important security role in the safety of CAVs. The automotive manufacturers who are pushing towards a future of CAVs are trying to determine the role of the drivers in controlling cyber incidents (Jadaan et al., 2017).

However, little research has been published regarding human behavior and SA in response to cybersecurity attacks on CAVs. As a result, there is insufficient information about how drivers perceive and react to cybersecurity attacks, and what possible ways there are to prevent or decrease the serious and potentially fatal outcomes.

1.2. Research Objectives

The objective of this study is to evaluate drivers' responses to unexpected cyberattacks, and to evaluate how cybersecurity knowledge affects SA during cyberattacks on automated driving. The results of the experiment seek to address the following research questions:

1. How do drivers respond to unexpected cyberattacks on automated and connected vehicles?
    a. For example, do drivers takeover control of their vehicle and brake, accelerate, change lanes or crash because of an unexpected cyberattack?
2. How does cybersecurity knowledge affect SA during cyberattacks on automated driving?
    a. For example, does increased cybersecurity knowledge lead to increased situation awareness while driving autonomously?
3. How does the type of cyberattack affect a driver's response?
    a. For example, does perception of consequences and past experience influence driver's decision to takeover control of their vehicle?

2. LITERATURE REVIEW

2.1. Automated and Connected Vehicles

Traffic congestion and vehicle crashes are considerable problems in large cities, which threaten road safety and increase commute time daily. A recent book from World Health Organization about global status report on road safety notes that road traffic crashes which is the main cause of death among people between the age of 5 and 29 causes over 1.2 million death each year (World Health Organization, 2015). According to the U.S. Department of Transportation, 93% of car crashes are attributed to human error (Singh, 2018). Congestion causes an average delay of 52 hours per year for the average commuter, which equates to $121 billion for the annual cost of delay and fuel (Schrank et al., 2012). During the congested condition up to 56 billion pounds of additional carbon dioxide (CO2) could be released into the atmosphere. (Schrank et al., 2012). Many countries and car manufacturers are looking for reliable solutions to road traffic problems such as deployment of some changes in roadway and vehicles design.

Autonomous vehicles are widely considered a viable solution to reducing collisions and road traffic. It is believed that autonomous vehicles (AVs) can prevent driver errors and reduce at least 40% of fatal crashes caused by fatigue, distraction, alcohol and/or drugs (Fagnant & Kockelman, 2015). The deployment of semi-autonomous technology is expanding, with implementation of supportive functions such as Forward Collision Warning, Pedestrian Safety, and Adaptive Cruise Control, which offer improved safety and efficiency to road traffic (Brar & Caulfield, 2017). For example, AVs can help decrease traffic congestion and fuel consumption by predicting trajectories of lead vehicles and increasing throughput of lanes and intersections (Fagnant & Kockelman,

2015). Also, implementation of automated systems provides benefits systems in other areas of transportation. For example, the replacement of human drivers in crash attenuators with automated truck-mounted attenuators has shown to improve work zone safety (Pourfalatoun & Miller, 2021). Society of Automotive Engineers International (SAE) classified the vehicle automation in 5-level standard. Operational functions of vehicle automation system are explained in Table 1 (Faisal et al., 2019).

Table 1. Vehicle Automation Levels (Faisal et al., 2019)

Level of Automation	**Automated Driving System**		**Human Driver**	
	Operational Function	*Capability*	*Operational Function*	*Capability*
Level 1 (most functions are controlled by driver)	Control: Lateral and longitudinal	In some driving modes	Localisation Perception Planning Management	In all driving modes
Level 2 (at least one driver assistant system is automated)	Control: Lateral and longitudinal	In some driving modes	Localisation Perception Planning Management	In all driving modes
Level 3 (driver is able to shift safety-critical functions to vehicle)	Control: Lateral and longitudinal Localisation Perception Planning	In some driving modes	Management	In all driving modes
Level 4 (fully-autonomous, but not in every driving scenario)	Control: Lateral and longitudinal Localisation Perception Planning Management	In some driving modes	n/a	n/a
Level 5 (fully- autonomous, vehicle's performance is equal that of human driver in every driving scenario)	Control: Lateral and longitudinal Localisation Perception Planning Management	In all driving modes	n/a	n/a

Despite the advances in vehicle automation technology, such as sensor integration, computer vision, and artificial intelligence, it is difficult to overcome problems

associated with human interaction with these sophisticated systems (Ebnali et al., 2020).

Like AVs, connected vehicles offer to provide safety for travelers and improve transportation network capacity (Jadaan et al., 2017). There are many benefits of connectivity of [autonomous] vehicles. Connected and autonomous vehicle (CAV) technology provides data transmission between vehicles (V2V) and between vehicles and infrastructure (V2I) for implementation of intelligent transportation systems (Petit & Shladover, 2014). Vehicle to Vehicle technology is illustrated in Figure 1 and Vehicle to Infrastructure technology in Figure 2.

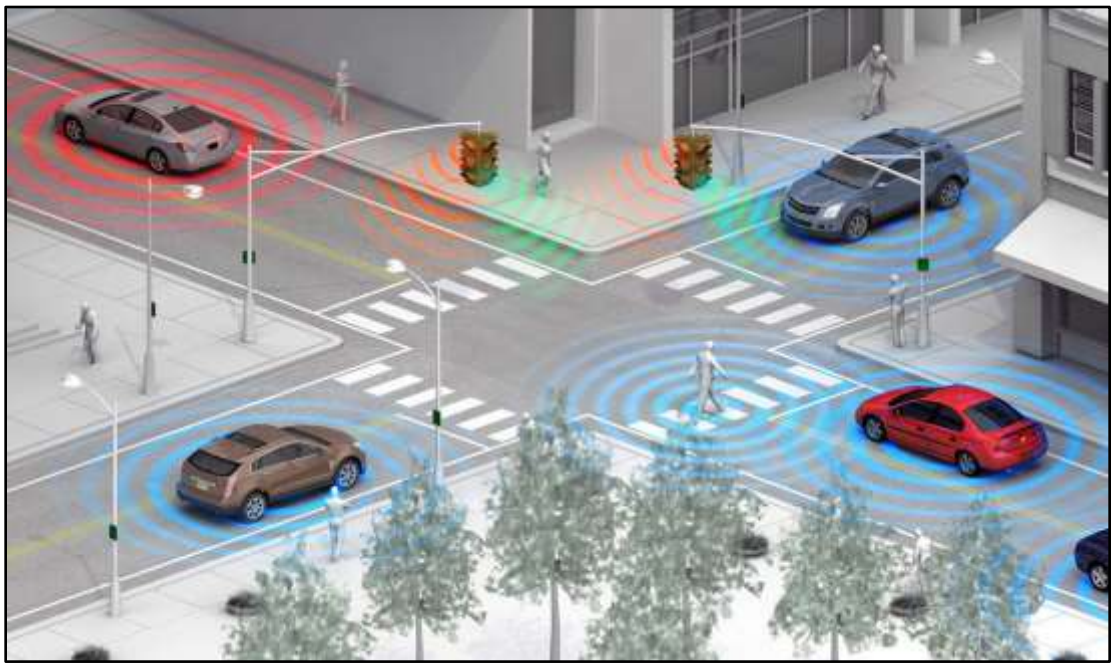


Figure 1. Vehicle to Vehicle (V2V) communication (Elkatib, 2018)

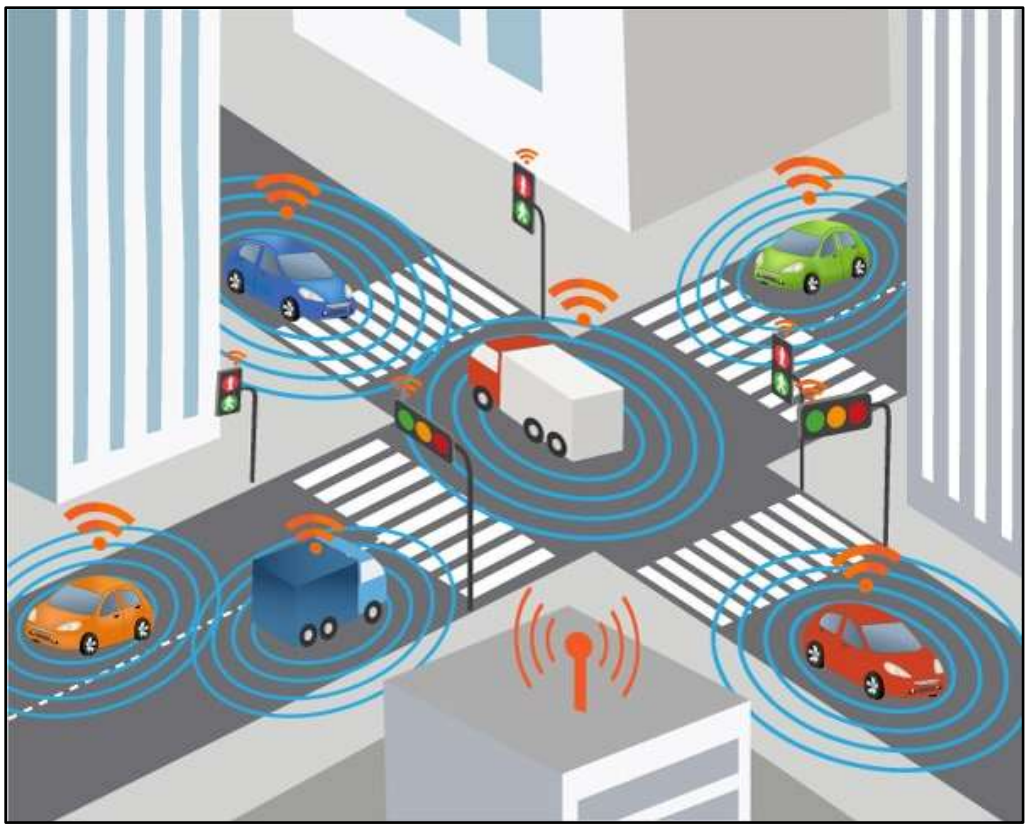


Figure 2. Vehicle to Infrastructure (V2I) communication (Schriber, 2017)

2.2. Connected and Automated Vehicles Challenges

However, it is important to consider the inevitable challenges that increased connectivity of systems, networks, vehicles, and infrastructure can create for drivers, other road users, and organizations. For example, smart cities are experiencing innovations in information technology, which provide economic opportunities, while also leading to threats to security and privacy. Further, humans, homes, cars, public and private transportation, and other systems are close to full connectivity, known as the Internet of Things (Elmaghraby & Losavio, 2014). With this vast number of connected systems and devices, the world is facing exceptional growth in cyberspace,

which makes it necessary to implement reliable cybersecurity to protect infrastructure and individuals (Arora, 2016).

2.2.1. Cyberattacks on CAVs

The interconnection of CAVs can increase safety, operational efficiency, and lead to environmental benefits, however this connectivity can also make CAVs vulnerable to cyberattacks and endanger both road and infrastructure safety (Khan et al., 2021). Some of the potential cyberattacks on CAVs include jamming, spoofing, denial-of-service (DoS), malware injection, blackholing, eavesdropping, Sybil attacks, and false information (Khan et al., 2021). Cyberattacks on connected and automated vehicles could be divided into different categories, as shown in Figure 3.

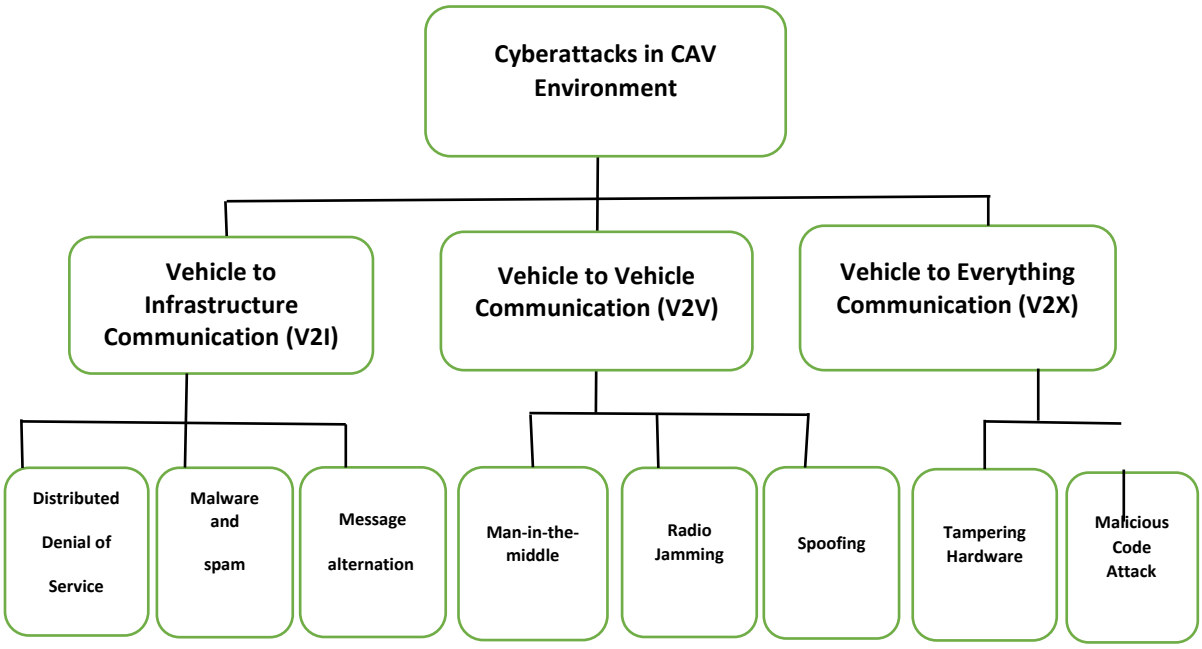


Figure 3. Attack Tree in Cyberattacks on CAVs Environment
(Islam et al., 2018; Khattak et al., 2021)

Three different categories of cyberattacks in Figure 3 are attacks on vehicle to infrastructure communication, vehicle to vehicle communication and vehicle to everything communication. All types of attacks in these 3 levels can have serious impacts on safety, security and privacy of drivers and vehicles (Khattak et al., 2021).

There are some research focusing on cyberattacks and their impacts by simulating, modeling or creating cyberattacks in real environment.

In a recent study with 10 participants, three attacks were created in a simulated driving environment to see how drivers would react to unexpected cyberattacks when driving in autonomous mode. The researchers also aimed to understand how drivers should be informed about cyberattacks and what they need to know in these situations. They programmed a horn sounding while there was not any other vehicle in the road, a check engine alert vehicle dashboard and loss of vehicles control. Results showed that even participants who are aware of what is happening during cyberattacks, they could misjudge the situation. Participants had very low knowledge about vehicle cyberattacks and their outcomes and thought happening cyberattacks on their vehicles is unlikely (Zhang et al., 2019).

In another study, researchers simulated numbers of significant attack scenarios to evaluate impact of cyberattacks on vehicle and road safety. In one of the scenarios, they deactivated the obstacle avoidance of the vehicle and changed the status of traffic light to unknown. The vehicle got confused with the attack and hit pedestrians and several cars on the road. In another scenario they simulated a Drive-By Download attack by which attacker can have access to secret data such as setting control and password of driver's smartphone and can inject malware to apps such as Google Maps.

In this simulated attack, once the connected car arrived at a crowded area in the road, researchers activated the malware, and the vehicle went off the defined road lane and hit another vehicle (Malik et al., 2020).

In a security research of Tesla autopilot, made an attack on steering system of the vehicle and learned by this attack they can take control of steering system without limitations when the car is parked or is in the ACC (Adaptive Cruise Control) mode (Keen Lab, 2019). In 2016, security researchers hacked a Mitsubishi Outlander plug-in hybrid electric vehicle by performing a man-in-the-middle attack and disabled the vehicle's theft alarm system (Lodge, 2016). In an attack by another group, the battery of a Nissan Leaf electric vehicle was drained by controlling the vehicle's heater through a vulnerability in the NissanConnect mobile application; Nissan disabled the application after that cyberattack (Eiza & Ni, 2017). An extended car-following model was created to evaluate the impacts of cyberattacks on traffic and the numerical results showed that security threats affect connected vehicles and can lead to traffic jams, delay, and rear-end collisions (Wang et al., 2018). Another study simulated three types of cyberattacks in a traffic environment to analyze the impact on CAVs, the results showed that inclusion of security in the design of CAVs can increase the safety and stability of CAVs significantly (Khattak et al., 2021).

2.3. Situation Awareness in Driving

Many automotive manufacturers and researchers are working with new technologies to secure CAVs from cyber threats, however, it is increasingly difficult to find a solution to prevent all cyberattacks as quantity and varieties of technologies in CAVs continues to grow (Zhang et al., 2019). In addition to cybersecurity technologies in connected

systems, it is important to consider the human-in-the-loop framework to evaluate behavior of humans who need to perform security-critical functions in response to cyberattacks (Cranor, 2008). As such, the way that drivers respond to unexpected cyberattacks plays an important security role in the safety of CAVs. The automotive manufacturers who are pushing towards a future of CAVs are trying to determine the role of the drivers in controlling cyber incidents (Jadaan et al., 2017).

Driving is a task that requires drivers to monitor the situational variables and react to vehicle speed, road, and traffic changes appropriately (Chaparro et al., 1999) and needs a proper level of situational awareness. Situational awareness (SA) is the perception of the information around to take proper actions to respond to the future event in a dynamic environment (Petersen et al., 2019). Operators may lose their situation awareness, surveillance, and skills while working with automated systems (Billings, 1997), which can cause human errors in the events beyond the capabilities of automation. In the driving domain, SA is defined as the perception of the relationship between a driver's goal, the vehicle state, road, infrastructure, other drivers, and objects on the road within a volume of time and space (Stanton et al., 2011). Therefore, adequate situation awareness is crucial for driver's performance, safety, and convenience even while driving in autonomous mode. CAV drivers need to remain in-the-loop and keep sufficient situation awareness to be capable of managing unexpected driving situations which automated systems are incapable of controlling due to their limitations (Merat et al., 2014). Therefore, it is hypothesized that drivers who are vigilant about the driving environment and aware of any changes in the vehicle or on the road, have a better opportunity to respond to cyberattacks.

Previous studies have evaluated the impact of situation awareness on drivers' reaction time to failure of AVs and its importance on safety. In a simulated driving study, Clark et al. (2017) found that participants who successfully performed a takeover during a failure of vehicle automation had higher SA compared to those who failed to manage the situation. Additionally, participants with higher SA had quicker reaction times than those with lower SA (Clark et al., 2017).

3. MATERIALS AND METHODS

A driving simulator study was conducted to evaluate driver response to four different cybersecurity attacks on autonomous vehicles. This study had IRB approval from the Colorado State University Institutional Review Board.

3.1. Participants

The study included 20 participants (10 male and 10 female). All participants had a valid US driver's license and had more than one year of driving experience. Participants were recruited through Colorado State University.

3.2. Driving Simulator

A National Advanced Driving Simulator (NADS) miniSim fixed-based driving simulator was used in this study. The Minisim is a PC-based driving simulator for simulation of a realistic automotive driving environment and is consists of a PC for, three front channel displays, an instrument panel display, USB steering wheel and pedals, 2.1 audio system, and a display for the operator/instructor. In this study, the driving display is composed of three 42-inch widescreen monitors (138° horizontal field of view) and a digital instrument panel. The NADS miniSim was used in this study is shown in Figures 4 and 5. The driving scenarios were developed specifically for this study. Simulator data was collected at 60 Hz.

Different MiniSim Tools were used to design the experiment and data collection are as follow:

- Tile Mosaic Tool (TMT)
- Interactive Scenario Authoring Tool (ISAT)

- MiniSim
- ndaqTools for Matlab

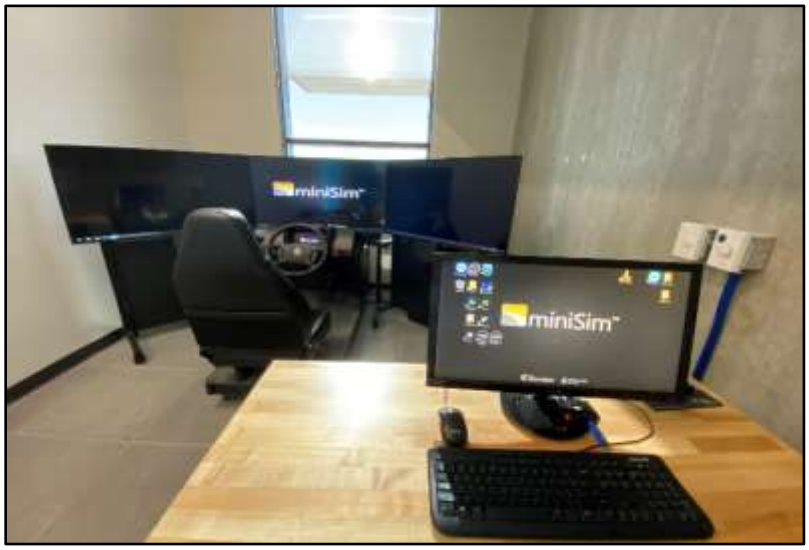


Figure 4. NADS miniSim driving simulator located in CSU Human Systems Lab

Figure 5. NADS miniSim driving simulator located in CSU Human Systems Lab

3.3. Driving Scenarios

The driving scenarios were created from scratch for this study by the researcher. The first step was to create the visual environment, which was created using the Tile Mosaic Tool (TMT) software. This software tool is part of the National Advanced

Driving Simulator (NADS) software suite. The TMT environment is shown in Figure 6. There were four different driving scenarios with identical roadway geometry and environments. The roadway was a 4-lane straight urban road without curves or hills.

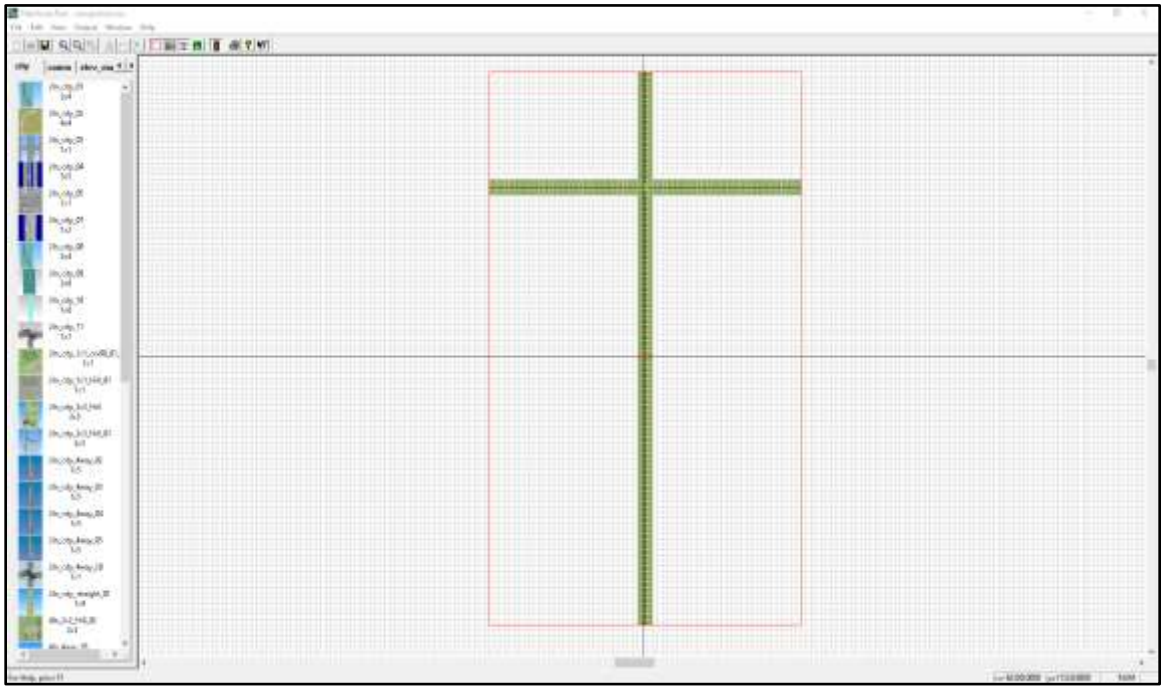


Figure 6. Tile Mosaic Tool (TMT)

Figure 7. Driving scenarios' roadway

After creating the visual environment, the scenario logic was created using The Interactive Scenario Authoring Tool (ISAT). ISAT was used for creating, modifying, and testing scenarios as well as designing the cyberattacks, vehicles, pedestrians, road

signs, objects on the road and roadside parking. In this program, I added when and how each cyberattack would occur, the timing of the traffic signal, and presence of other road users. Figure 8 and Figure 9 show the ISAT environment.

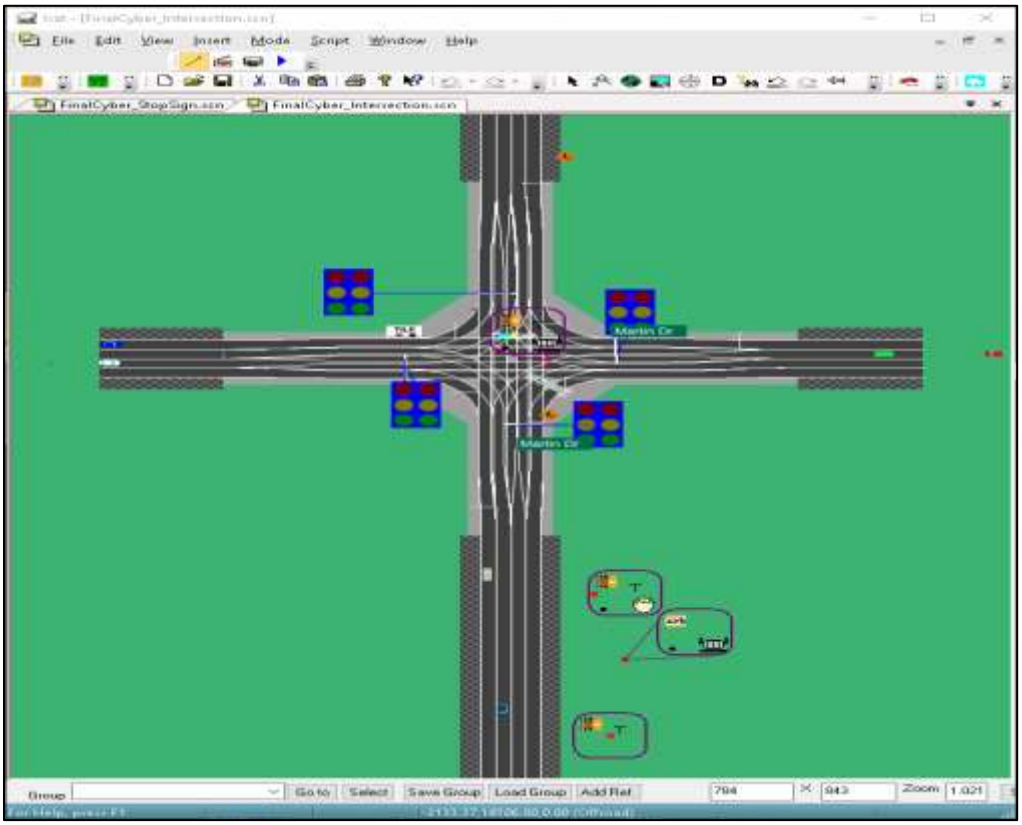


Figure 8. ISAT environment of designing an intersection

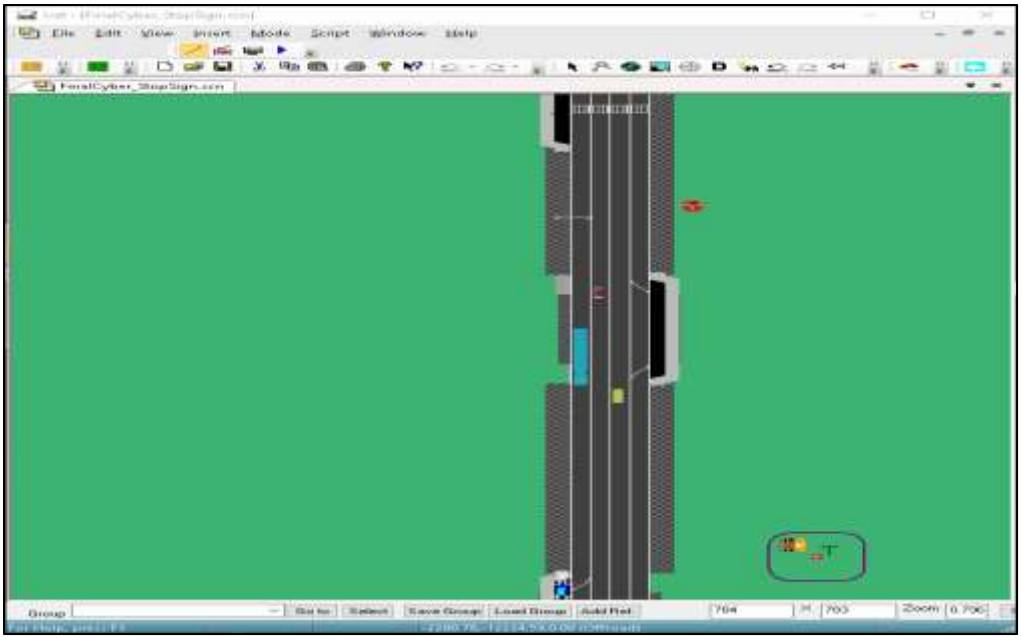


Figure 9. ISAT environment of designing the 4-lane roadway

There were four experimental drives, each about 4-minutes long, and a 2-minute practice drive. The driving environments were designed to simulate a typical roadway with light traffic, some pedestrians, and some vehicles parallel parked along both directions of travel.

The vehicle simulated an SAE Level 2 partially-autonomous vehicle. Participants were asked to set the vehicle speed to 55 mph and activate the Adaptive Cruise Control as well as Lane Keeping modes at the beginning of each. For each drive, we programmed a different cyberattack to occur in the last one minute of the drive. Participants were able to takeover control of the vehicle by braking, accelerating, or changing lanes.

3.4. Cyberattacks

There were four different cyberattacks, one in each driving scenario (see Figure 1). Each attack represented a possible attack that could happen on current vehicle

technology. Participants were randomly assigned to the order of the drives to eliminate priming effects.

Bright Light Attack (cyberattack to vehicle). At 204 seconds into the drive until the end of the drive, a bright light appeared on the vehicle's windshield; it would appear solid for 5-seconds every about 4 seconds. The designed bright light blocked the driver's forward view of the road and blinded the vehicle's sensors. After about 30-seconds of the flashing light, the vehicle would collide with a pedestrian, unless the participant stopped the vehicle during the attack. This scenario represented sensors being blinded through either extreme sun exposure or a nefarious bright light aimed to blind the vehicle sensors. The objective was to see if participants would continue to trust that the vehicle's sensors would accurately control the vehicle, despite the participant losing visual sight of the road. Figure 10 and Figure 11 show the bright light attack from driver's view in the vehicle's windshield. The location of pedestrian in the bright light scenarios is shown in Figure 12.

Figure 10. Driver's view to the front road before bright light attack

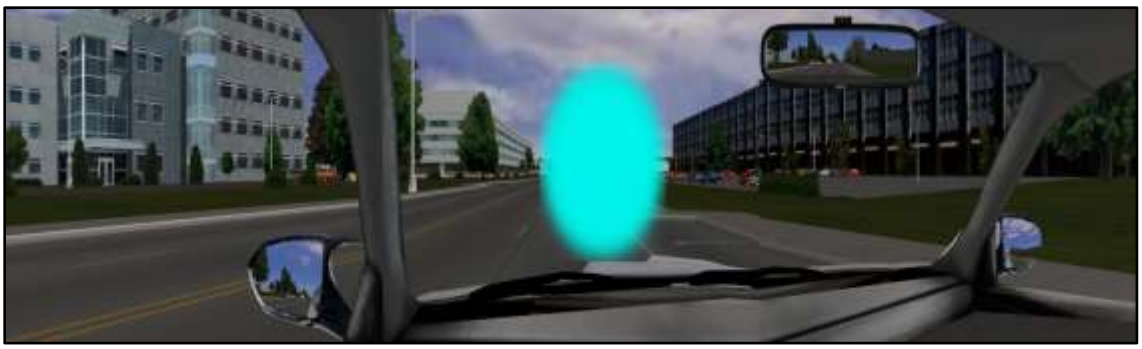


Figure 11. Driver's view to the front road during bright light attack

Figure 12. Road worker in the roadway at bright light scenario

Stop Sign Attack (cyberattack to infrastructure). In the stop sign scenario, we designed a manipulated stop sign with stickers placed on the sign to interfere with the vehicle's classification of the sign. The stop sign was located before a sidewalk without any pedestrians present. This scenario replicated the stop sign attack presented in Eykholt et al. (2018). The vehicle was programmed not to recognize the stop sign, and the objective was to evaluate if participants noticed that the vehicle was not sensing the stop sign and takeover control. Figure 13 shows the roadway when the driver reaches the manipulated stop sign in Stop Sign scenario.

Figure 13. Manipulated stop sign in Stop Sign scenario

Instrument Panel Attack (cyberattack to vehicle). In this driving scenario we programmed an attack on the instrument panel of the vehicle at 190-seconds into the drive. The instrument panel turned off and on (i.e., went black) repeatedly until the end of the drive. The objective of this scenario was to see if the participants would consider this enough of a threat to takeover control. Figures 14 and 15 show the instrument panel form driver's view during the instrument panel cyberattack.

Figure 14. Cyberattack on instrument panel in the seconds it is turned on

Figure 15. Cyberattack on instrument panel in the seconds it is turned off

Intersection Attack (cyberattack to infrastructure). At the end of this scenario, there was a 4-legged signalized intersection. The traffic signals for all approaching lanes were designed to change every 2-seconds from green to red to green, etc. There were vehicles entering the intersection from the other approaches, and there were at least two vehicles in the middle of the intersection when the participants approached. The drive was programmed to end when the participants entered the intersection or stopped before the intersection in response to the cyberattack. The objective was to evaluate if the participants took over control during this infrastructure attack. The traffic lights during cyberattack are shown in Figures 16 and 17.

Figure 16. Driver's View to Green Traffic Lights in Intersection Attack

Figure 17. Driver's View to Red Traffic Lights in Intersection Attack

3.5. Procedure

At the start of the study, participants signed a consent form and were told the purpose of the study was to evaluate driving performance in an autonomous driving simulator. They were intentionally not told about the cybersecurity focus of the study. Then, participants were told the vehicle automation simulated market available autonomous driving, with lateral and longitudinal control, but they were in charge of monitoring the driving environment and to takeover control if needed. Participants were then given a two-minute practice drive to become familiar with the simulator and automation. After the practice drive, participants completed the four experimental drives in a random

order. After each of the experimental drives, participants responded to a SAGAT questionnaire consisting of four questions. At the end of the last drive participants also completed a cybersecurity knowledge survey.

3.6. Situation Awareness Survey

Participants' situation awareness was evaluated using a situation awareness global assessment (SAGAT) questionnaire. The questionnaires were given to participants at the end of each drive. Each questionnaire consisted of four questions about what happened or what they saw during the drive. SAGAT questions were designed so that they cover all the three different levels of situation awareness including perception, comprehension, and projection. By SAGAT participants could easily report what they noticed and perceived in the last driving scenario. SAGAT not only identifies whether participants perceived the objects and elements, but it measures how much information they kept in their mind and if the information has been stored correctly (Endsley, 1996).

Questions in level 1 SA perception level which is the lowest level of situation awareness concentrates on the elements in the driving environment such as the location of pedestrians, vehicles as well as the color of these elements in the environment. Examples of perception level questions in the study are listed below.

- What was the color of the vehicle directly behind you prior to stopping the simulation?

  A. Gray B. Red C. Blue D. Not sure

- Where was the last parked vehicle located just before the end of the drive?

A. On the left-side of the road

B. On the right-side of the road

C. There was no vehicle parked

D. Not sure

The second level of situation awareness comprehension refers to a combination of elements in the environment to comprehend the situation. Comprehension level integrates the perceived information from level 1 SA and helps to identify the significance of elements for desirable goals (Fricker, 2013) . Examples of comprehension level questions in the study are listed below.

- What type of vehicle was last parked along the side of the road?

A. Police B. Truck C. Taxi D. Not sure

- Which side of the road were you driving when the simulation ended?

A. 1

B. 2

C. 3

D. Unknown

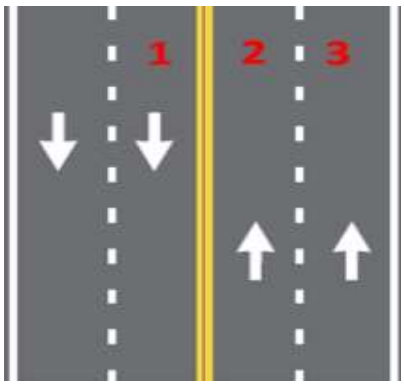


Figure 18. Road Lanes

Level 3 situation awareness which is highest level of SA aims to understand how participants can predict the future status of current situation in driving environment. Examples of level 3 SAGAT questions in the study are listed below.

- If you had kept driving, where would the pedestrian have been when you arrived at crosswalk?

A. Just entering the crosswalk

B. In the crosswalk

C. Finished walking through the crosswalk

D. Not sure

- How long would it take to reach the next stop sign at the speed you were driving before you stopped?

A. Less than 5 seconds

B. 5-20 seconds

C. 20-30 seconds

D. Not sure

One of the four questions for each scenario specifically aimed at capturing if the participants noticed the cyberattack, without specifically indicating that an attack occurred. For example, in the stop sign scenario, the question asked:

- What unusual situation did you notice during the last 1 minute of the drive?

A. Traffic light was off

B. Animal on the roadside

C. Physical change of stop sign

D. Not sure

There were two metrics analyzed for the SAGAT data: *(1)* total SAGAT score for each participant on each drive (i.e., number correct out of four) and *(2)* whether they got the question correct about being aware of the attack (i.e., correct/incorrect).

3.7. Cybersecurity Awareness Survey

At the end of the experiment participants were asked to respond to an online survey in Qualtrics. The survey consisted of 18 questions including inquiry of age, gender, education level, knowledge of various general cybersecurity concepts and experience with automated vehicle technology. Some questions aimed to evaluate participant's awareness about cybercrimes such as denial of service, spoofing, man-in-the-middle, password sniffing, and phishing to understand if there is a relationship between level of familiarity with these terms and their situation awareness and performance in the experiment. We also wanted to evaluate how high level of protection against cybercrimes can result in higher situation awareness and better performance in the experiment. In the cybersecurity awareness survey participants also were asked to indicate their level of experience with autonomous vehicle technologies such as blind spot detection, adaptive cruise control, lane keeping assist, automatic braking, self-parking, and self-driving. Examples of cybersecurity knowledge survey questions are listed below:

- How important do you think the following are to ensure security?

	Extremely	Moderately	Somewhat	Slightly	Not at all
Firewall					
Anti-Virus software					
Password manager					
Encryption					

- How familiar are you with the following technologies?

	Extremely	Moderately	Somewhat	Slightly	Not at all
Connected Vehicles					

Vehicle-to-Vehicle
(V2V)
Vehicle-to-
Infrastructure (V2I)
Vehicle-to-
Everything (V2X)

- Typically, after an online activity requires you to use a password, what do you do?

  A. Logoff and close browser

  B. Just logoff

  C. Just close browser

  D. Do not log off or close browser

3.8. Driving Performance Measures

Participant takeover responses were captured through the driving simulator to evaluate how they responded to each cyberattack. The time/location of the cyberattack in each scenario was tagged and driving performance measures were analyzed during each cyberattack. The driving performance measures analyzed were vehicle speed and steering wheel angle, which were used to determine if and how they took control of the vehicle during the attack.

3.9. Data Analysis

Data analysis was conducted to compare participant driving response, situation awareness, and general cybersecurity knowledge. For this, multi-way Analysis of Variance (ANOVA) and Mann-Whitney U-tests were performed. To test the ANOVA

assumptions, we used the Shapiro-Wilk test for normality and Levene test for homogeneity of the variance. Statistical significance was evaluated at $\alpha = 0.05$

4. RESULTS

4.1. Participants

The study consisted of 10 males and 10 females. The age range of participants was 21 - 48 years old (Mean = 31.3, SD = 7.09). Among the 20 participants, seven had a master's degree, two an associate degree, nine a bachelor's degree, and two had a high school or equivalent degree. There were two participants with a degree or job relevant to computer science, five who had taken some training or courses relevant to computer science, six with some informal experience, and seven who had no experience with computer science. Figure 19 and Figure 20 show the pie charts for participants' education level and computer programming experience respectively.

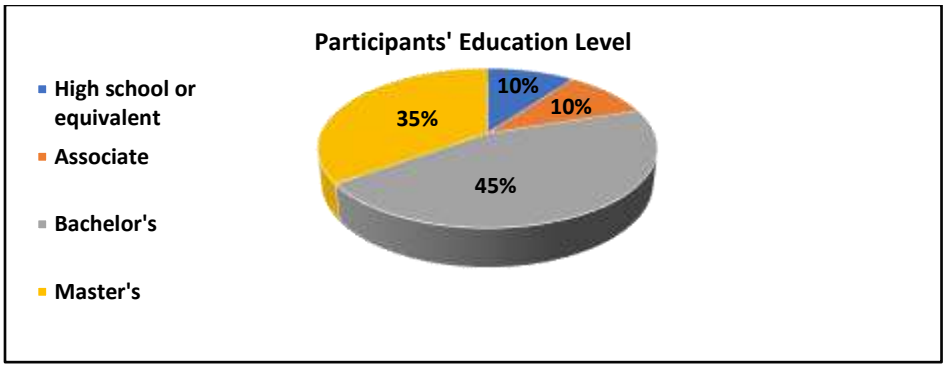


Figure 19. Participants' Education Level

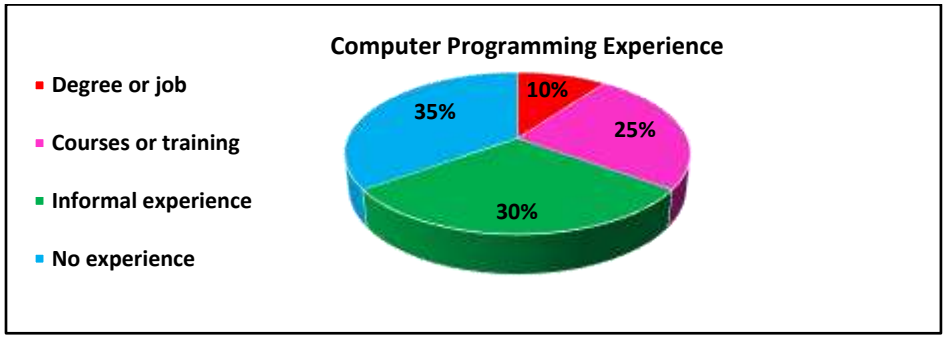


Figure 20. Participants' Computer programming experience

4.2. Driving Response and Awareness to Cyberattacks

Participant driving responses to the cyberattacks including brake, change of lane and stop as well as number of collisions were recorded through the driving simulator for all driving scenarios. We considered stopping the vehicle as the safest response to the cyberattack in all drives because the vehicle was compromised and best not continue driving it. Further, a complete stop response was most appropriate for the four attacks, as an evasive maneuver or another similar behavior would not have overridden the cyberattack. Figure 21 shows the number of different reactions to cyberattacks in different scenarios. As it is shown in the bar plot in Figure 21 in the intersection scenario, more participants responded to cyberattack in the safest way compared to other 3 scenarios.

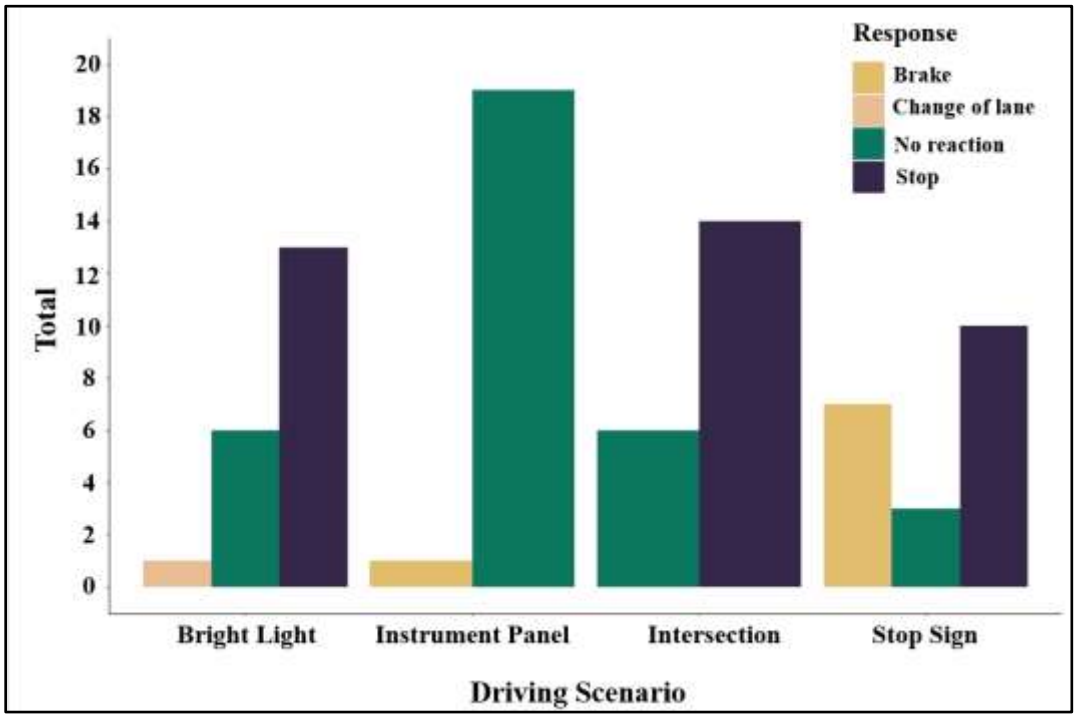


Figure 21. Participants' reaction to cyberattacks

Bar plots in Figures 22.a and 22.b show cause of collisions during the entire experiment and in different driving scenarios. As Figure 22.a shows, the majority of crashes (75%) were caused by cyberattacks.

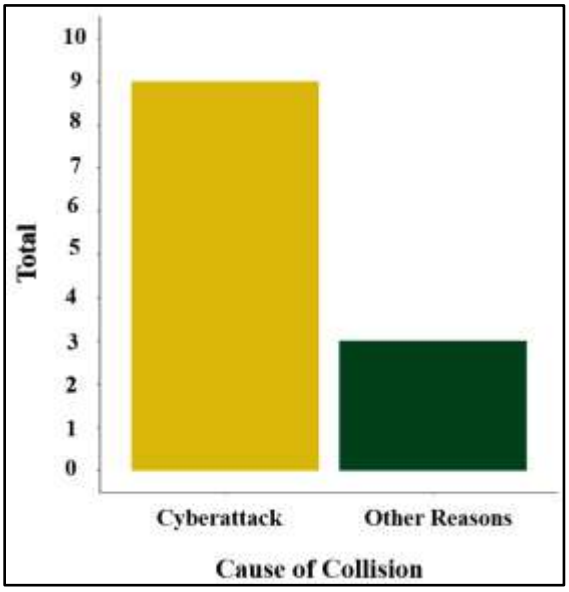


Figure 22.a Cause of Collisions During the Experiment

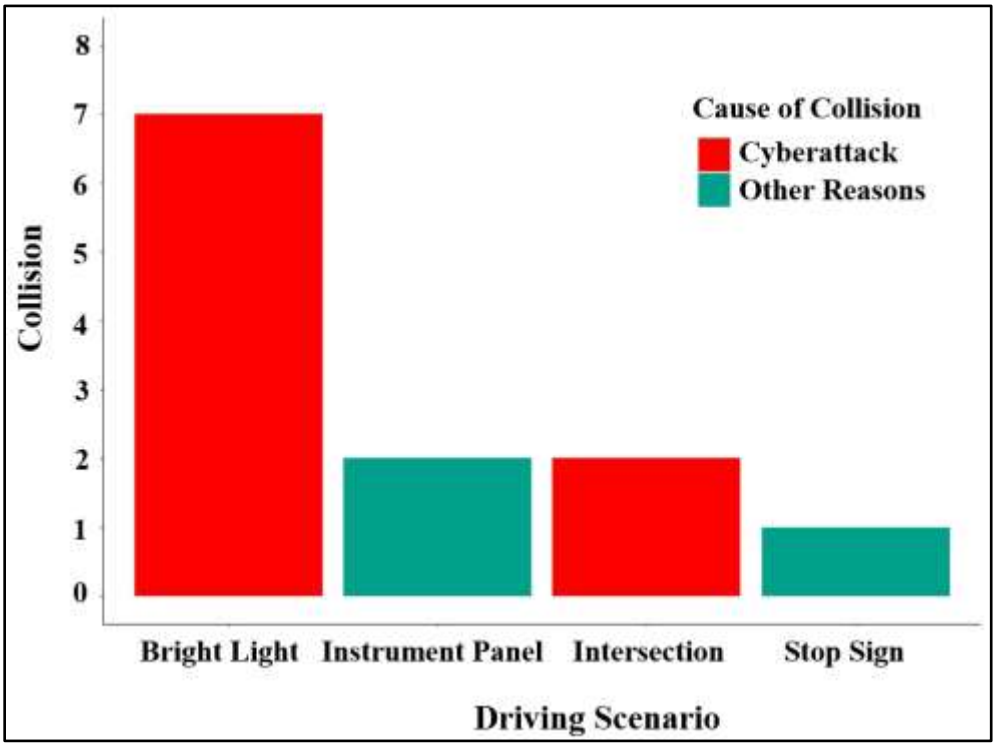


Figure 22.b. Cause of collisions in driving scenarios

Participants' decision to takeover control and stop the vehicle was also compared with their response to the SAGAT question evaluating their awareness of the specific attack (see Table 2). Results show that in all driving scenarios most participants (more than 75%) were aware of the attack. In other words, most of the participants recognized the unusual situation that happened during the drives. However, there were many participants (30% to 95% depending on the scenario) who did not stop the vehicle as a response to the attacks despite being aware that the attack was occurring. For example, in the instrument panel scenario, 19 (95%) participants were aware of the attack, yet none of them stopped the vehicle.

Table 2. Driver responses to cyberattacks, N (%)

Awareness of Attack	**Driving Response**	**Bright Light**	**Stop Sign**	**Instrument Panel**	**Intersection**	**All Driving Scenarios**
Aware	Stopped	12 (60%)	7 (35%)	0 (0%)	13 (65%)	32 (40%)
	Did Not Stop	7 (35%)	8 (40%)	19 (95%)	6 (30%)	40 (50%)
	Total	19 (95%)	15 (75%)	19 (95%)	19 (95%)	72 (90%)
Not Aware	Stopped	1 (5%)	3 (15%)	0 (0%)	1 (5%)	5 (6%)
	Did Not Stop	0 (0%)	2 (10%)	1 (5%)	0 (0%)	3 (3%)
	Total	1 (5%)	5 (25%)	1 (5%)	1 (5%)	8 (8%)

4.3. Situation Awareness During Drives

The total situation awareness for each participant was computed for each scenario using the SAGAT data, summary data on this is provided in Table 3. The possible scores for SAGAT could range from 0 (lowest SA) to 4 (highest SA). The bright light scenario had the highest average participant SA (2.55) and the stop sign scenario had the lowest average SA (1.60).

Table 3. Situation awareness during drives (out of 4)

Scenario	**Scores, N (%)**					**Summary**	
	0	1	2	3	4	Average	Std Dev
Bright Light	0 (10%)	2 (35%)	7 (45%)	9 (5%)	2 (5%)	2.55	0.82
Stop Sign	2 (0%)	7 (20%)	9 (60%)	1 (15%)	1 (5%)	1.60	0.94
Instrument Panel	0 (0%)	4 (50%)	12 (30%)	3 (20%)	1 (0%)	2.05	0.76
Intersection	0 (%)	10 (%)	6 (%)	4 (%)	0 (%)	1.70	0.80

A Shapiro-Wilk test was used to test for normality and indicated that the SAGAT scores for each scenario were not normally distributed. Hence, a Mann-Whitney U-test was performed to evaluate the difference between the SAGAT medians for the different driving scenarios. Results from the Mann-Whitney U-test suggest that participants' situation awareness in the bright light scenario were significantly different than in each of the other scenarios. There were no significant differences between SAGAT scores for the other scenarios (see Table 4).

Table 4. Statistical comparison of SAGAT between scenarios.

Scenario…	Bright Light	Stop Sign	Instrument Panel	Intersection
Bright Light	--	p = .0017	p = .0415	p = .0036
Stop Sign	--	--	ns	ns
Instrument Panel	--	--	--	ns
Intersection	--	--	--	--

4.4. Cybersecurity Awareness Survey and Responses

Below are the responses to Qualtrics survey which participants completed at the end of the experiment. Questions in cyber security knowledge survey were designed to evaluate participants' awareness in three different areas including their cybersecurity knowledge, their protection against cyberthreats and their knowledge of connected and automated vehicles. Participants' responses to these questions are shown by figures or tables to provide more clarification of the results.

4.4.1. General Cybersecurity Knowledge

Have you ever attended a cyber security awareness event or training class?

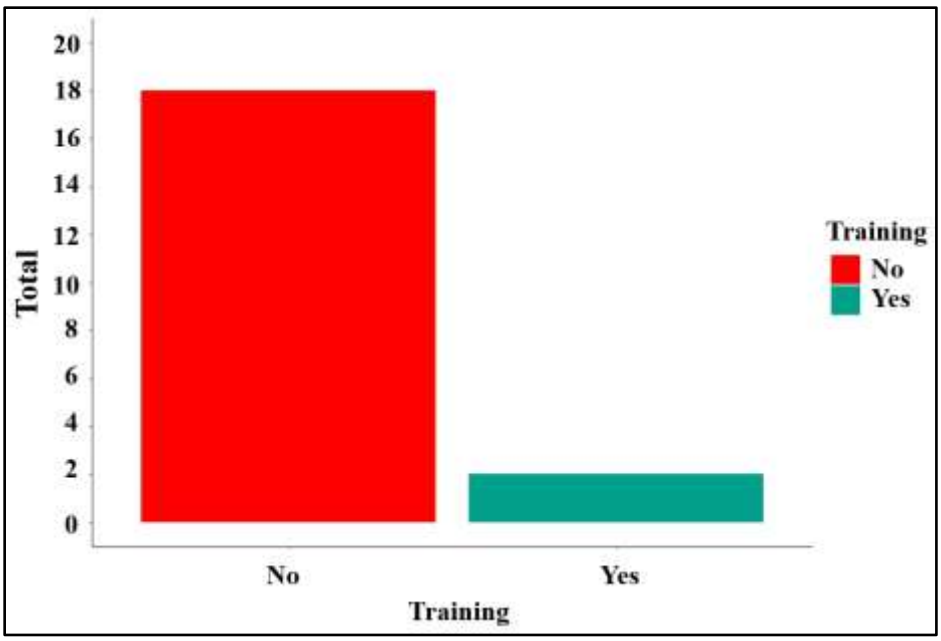


Figure 23. Participant's attendance to cybersecurity training classes/events

Do you know what scam emails are and how to recognize them?

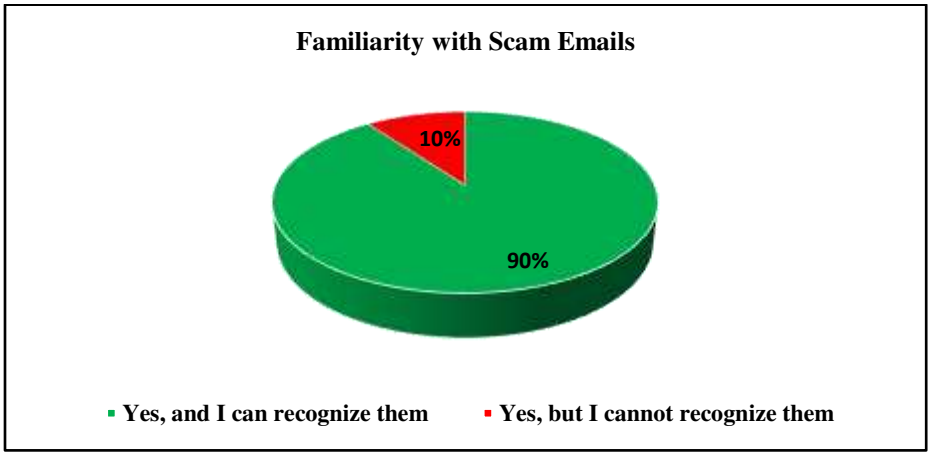


Figure 24. Familiarity with scam emails

How familiar are you with the following terms?

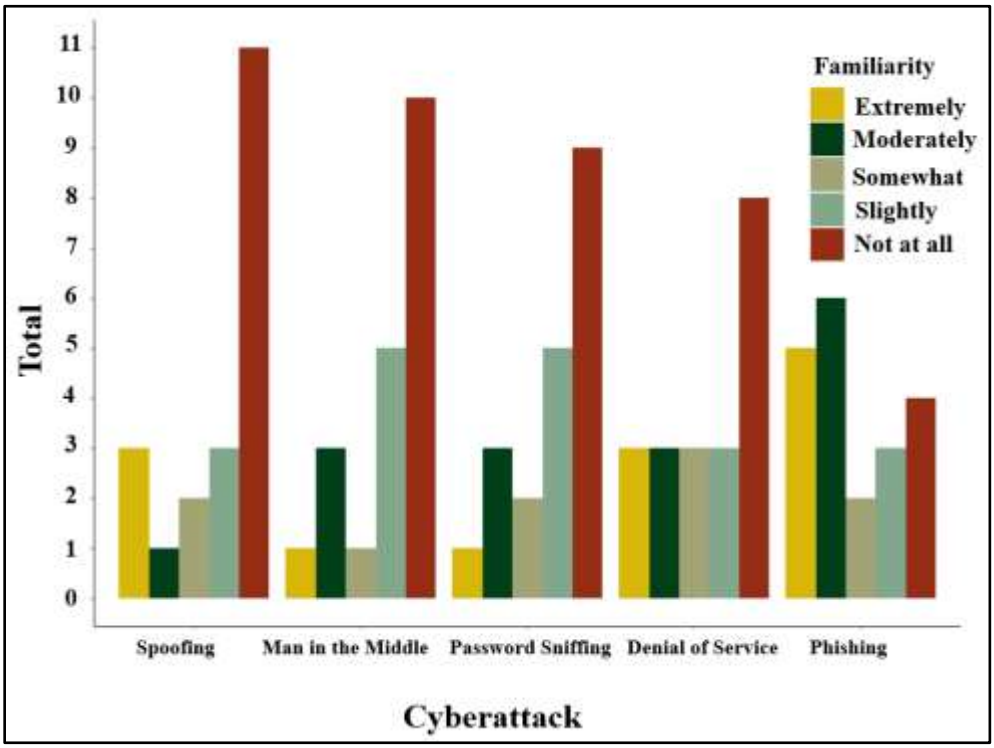


Figure 25. Familiarity with Cyberattacks

How important do you think following are to ensure security?

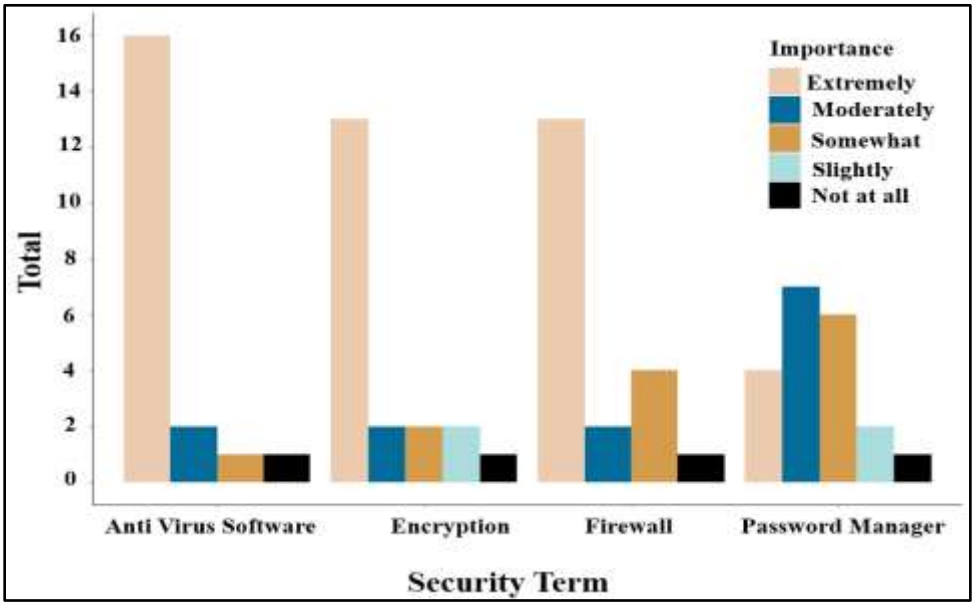


Figure 26. Importance of security tools

How often do you think someone should change their email password?

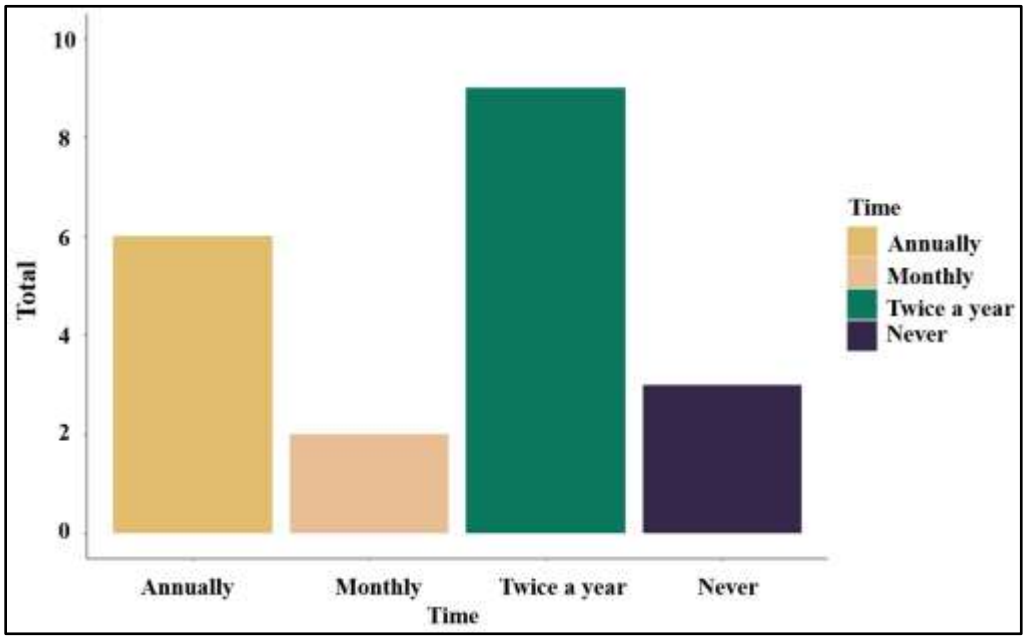


Figure 27. Change of email password

If a public Wi-Fi network (such as in an airport or cafe) requires a password to access it, is it generally safe to use that network for sensitive activities such as online banking?

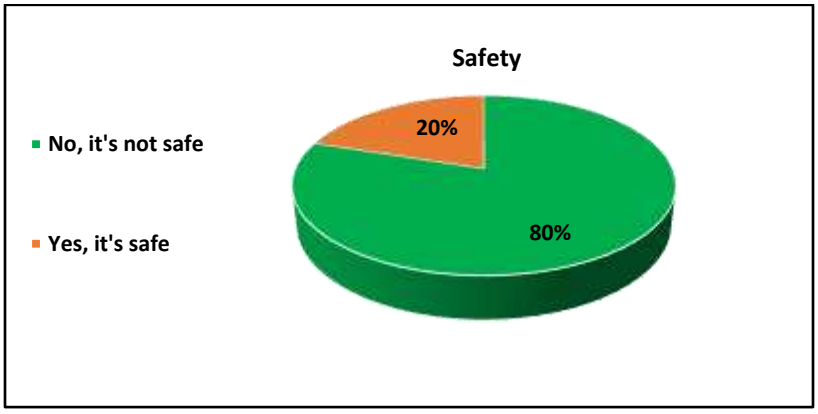


Figure 28. Safety of using public network for sensitive online activities

4.4.2. Protection against cyber threats

How protected do you feel against the following cyber-crimes?

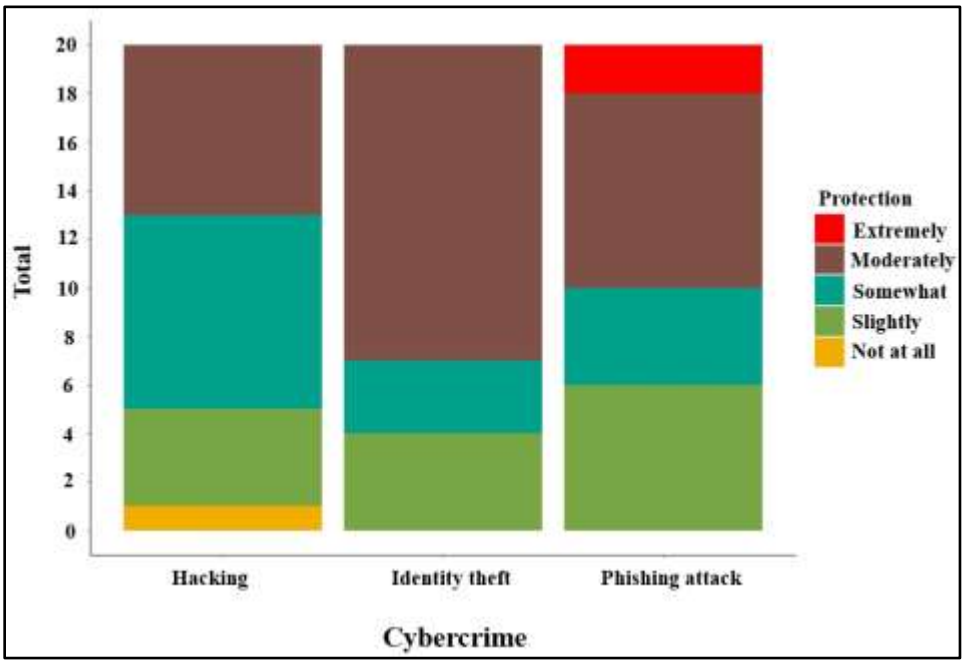


Figure 29. Protection against cybercrimes

Typically, after an online activity requires you to use a password, what do you do?

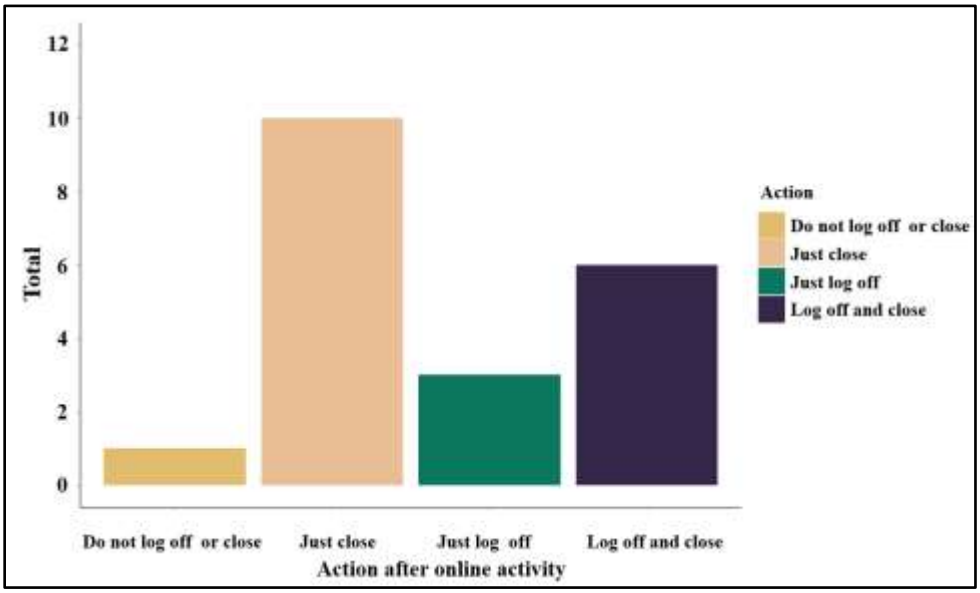


Figure 30. Precaution after online activity

Do you open emails you receive from unfamiliar sources?

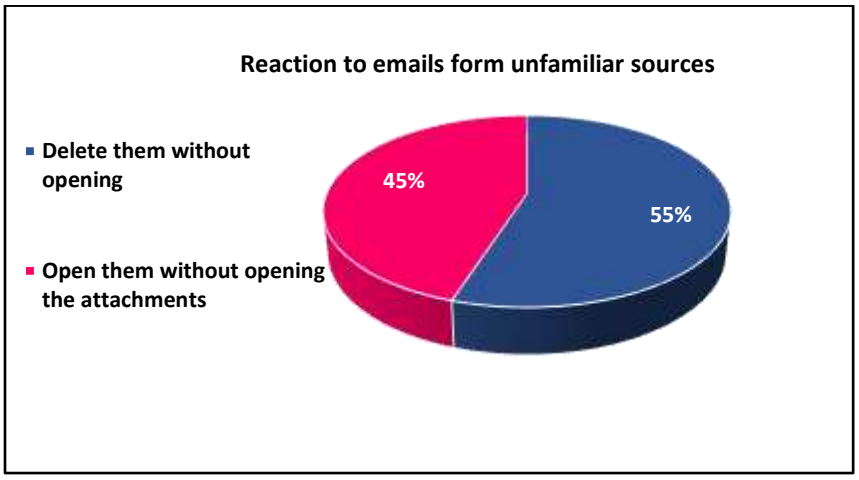


Figure 31. Reaction to emails from unfamiliar sources

Would you log in into your bank account from a public computer (e.g., library, cafe, etc.)?

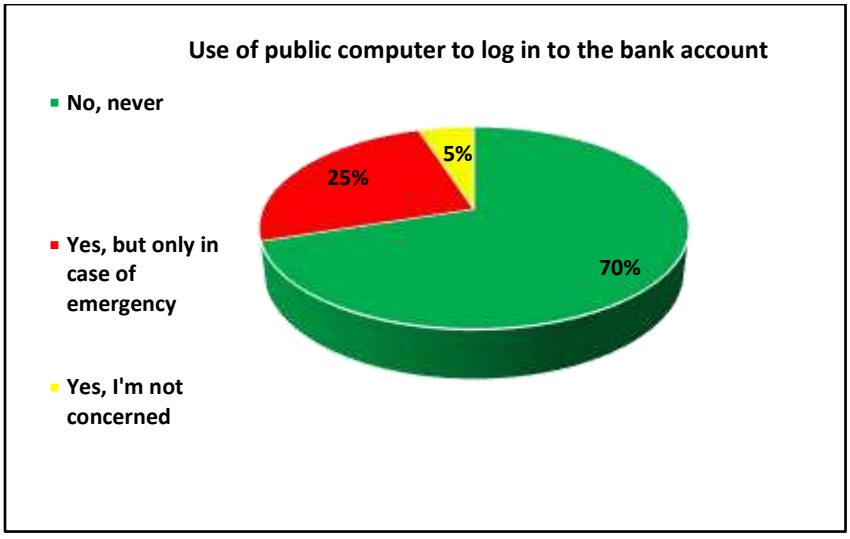


Figure 32. Use of public computer to log in to the bank account

4.4.3. Connected and Autonomous Vehicles

How familiar are you with the following terms?

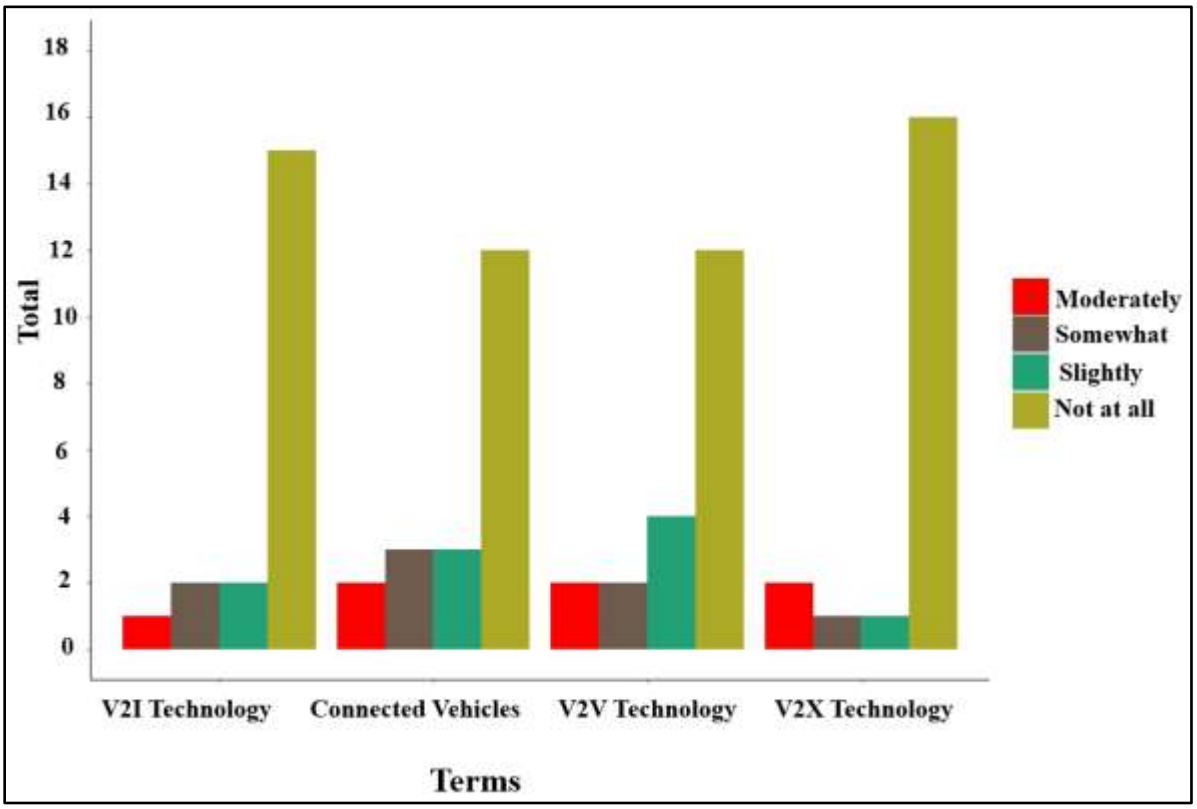


Figure 33. Familiarity with vehicle communication technologies

Which best describes your experience with the following autonomous vehicle technologies?

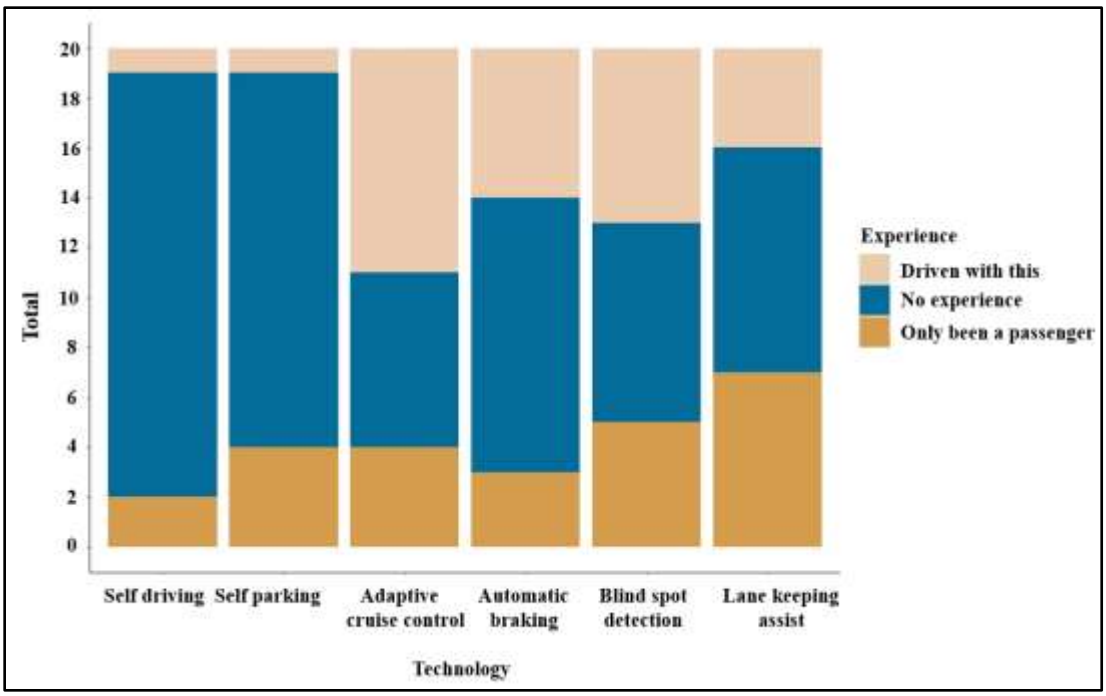


Figure 34. Experience with autonomous vehicle technologies

How concerned are you about cyber threats to autonomous vehicles?

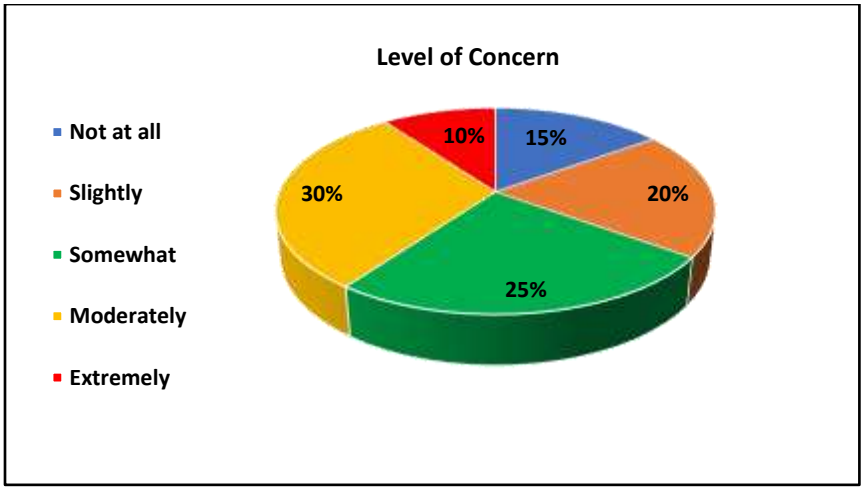


Figure 35. Concern level about cyber threats to automated and connected vehicles

4.5. Comparison of SAGAT with Cybersecurity Awareness

Multi-way ANOVAs were used to evaluate the relationship between participants' cybersecurity awareness (as measured in the cybersecurity knowledge survey) and their

SAGAT scores in each driving scenario. Post hoc analysis, using Tukey Honest Significant Difference (HSD) tests, were used to further evaluate the differences between factor levels.

4.5.1. Familiarity with Cybersecurity Terms

Participants were asked to rate their familiarity with common cybersecurity terms on a 5-point Likert scale from 1 (not familiar with at all) to 5 (very familiar with). The terms were man-in-the-middle, spoofing, and vehicle-to-everything (V2X) technology. A two-way ANOVA was performed for each scenario for the effect of familiarity with man-in-the-middle and spoofing on average SAGAT. Since V2X technology isn't necessarily a cybersecurity term, this was evaluated as its own one-way ANOVA for each of the four scenarios. Overall, the results showed that participants with greater familiarity with the terms had higher situation awareness during the bright light, instrument panel, and intersection drives.

Specifically for the bright light scenario, there was a significant effect of familiarity of man-in-the-middle ($F(4, 7) = 5.99$, $p = .02$) and no significant effect ($p > .05$) of familiarity of spoofing or V2X technology. Based on the Tukey HSD test, a higher familiarity of man-in-the-middle was associated with a higher SAGAT score. For the instrument panel scenario, there was a significant effect of familiarity with spoofing $F((4, 11) = 1.2$, $p = .01)$, where the Tukey HSD test indicated a higher familiarity of spoofing was associated with a higher SAGAT score. For the intersection scenario, there was a significant effect of familiarity of spoofing ($F(4, 7) = 4.6$, $p = .03$), where once again the mean SAGAT score tended to be higher for increased familiarity with spoofing. Additionally, there was a significant effect of familiarity of vehicle-to-

everything (V2X) technology ($F(1, 16) = 5.6$, $p = .03$), with more familiarity associated with higher SAGAT scores.

4.5.2. Perceived Importance of Cybersecurity

Participants were asked how important they considered firewall and encryption for ensuring security. This was asked on a 5-point Likert scale, from 1 (not important at all) to 5 (very important). To analyze this, a two-way ANOVA was conducted for each scenario to evaluate differences in SAGAT scores based on perceived importance of security features. Overall, SA was higher in the bright light and stop sign scenarios for participants who considered these security systems important.

In the bright light scenario, there was a significant effect of the level of importance of firewall ($F(2, 12) = 3.9$, $p = .04$), but no significant effect ($p > .05$) of encryption. Based on the Tukey HSD test, a higher level of perceived importance of firewall was associated with a higher SAGAT score. For the stop sign scenario, there was a significant effect for the level of perceived importance of encryption ($F(2, 13) = 4.64$, $p = .03$), but not for perception of firewall. The mean SAGAT score tended to be higher for increased perception of the importance of encryption.

4.5.3. Perceived Protection from Cyber Crimes

Lastly, participants were asked how protected they felt against hacking and identity theft, on a scale from 1 (not protected at all) to 5 (extremely protected). Similarly, a two-way ANOVA was conducted for each scenario on SAGAT scores. Participants who reported feeling protected against cyber-crimes had higher situational awareness during the stop sign drive. Specifically, there was a significant effect of perceived

protection from identity theft ($F(2, 11) = 6.6$, $p = .01$) on average SAGAT score, and no significant effect ($p > .05$) for level of perceived protection against hacking. The Tukey HSD test showed that mean SAGAT score tended to be higher for higher reported protection against identity theft.

4.5.4. Summary of ANOVAs on SAGAT by Cybersecurity Awareness

A summary of the results for the statistical tests described above is provided in Table 5, where in all cases of statistical significance, increased knowledge on the respective topic translated to higher SAGAT scores.

Table 5. Statistical significance between SAGAT and cybersecurity awareness

Cyber Knowledge		**Bright Light SAGAT**	**Stop Sign SAGAT**	**Instrument Panel SAGAT**	**Intersection SAGAT**
How familiar are you with…					
	Man-in-the-Middle	.02	ns	ns	ns
	Spoofing	ns	.03(ns)	.01	.03
	V2X Technology	ns	ns	ns	.03
How important are each of these for ensuring security…					
	Firewall	.04	ns	ns	ns
	Encryption	ns	.03	ns	ns
How protected do you feel against…					
	Hacking	ns	ns	ns	ns
	Identity Theft	ns	.01	ns	ns

5. CONCLUSIONS

5.1. Discussion

Many vehicle manufacturers are focusing on connectivity to make CAVs capable of communicating with nearby vehicles and infrastructure regarding the vehicles' position and other information. However, as a result, connected vehicles are at risk of cyberattacks that can lead to serious consequences, such as traffic congestion and crashes (Khattak et al., 2021). To enhance the safety of CAVs, it is important to investigate the factors that can help drivers respond to cyberthreats immediately and appropriately. In automated and connected vehicles, like many other automated systems, a high situation awareness of the user enables the human to recognize the malfunction, and in this application, the cyberattack on the automotive system immediately. However, previous literature that evaluates situation awareness of drivers in automated vehicles have found that drivers have lower SA when driving in automated modes (Merat & Jamson, 2009). This current study builds on that research by further using SA and other potential factors (i.e., cybersecurity knowledge) to evaluate cyberattack events in automated vehicles. We evaluated recognition of cyberattacks by drivers and the importance of cybersecurity knowledge on their situational awareness while driving in autonomous mode. An important finding of our work is the differences in participants' responses to cyberattacks and their SA scores in different driving scenarios.

Results from the SAGAT questionnaires indicate that in all driving scenarios the majority of participants were aware of the unusual situation (i.e., cyberattack), since they correctly answered the question for each scenario related to the cyberattack.

However, fewer participants performed the appropriate driving response (i.e., takeover control) to the cyberattacks. For example, in the stop sign scenario, 75% of the participants noticed that the stop sign was maliciously manipulated. However, only half of the participants who noticed the stop sign manipulation stopped the vehicle. Meanwhile, three people did not notice the stop sign manipulation, but noticed that the AV was not going to stop and chose to intervene by manually stopping the vehicle themselves. This suggests that there is an overall confusion on vehicle automation limitations and cybersecurity threats. This is of immediate concern, as previous researchers have shown cyber threats to infrastructure can adversely impact vehicles currently on the road today. Eykholt et al. (2018) performed a field test and showed that a few black and white stickers on a stop sign, that would not affect a human's perception, can cause a moving vehicle to misclassify a stop sign 84.8% of the time. In another cyber-physical attack, Keen Security Labs found that the Tesla autopilot's lane recognition fails to correctly identify lane boundaries when interference stickers are placed on the road (Keen Lab, 2019).

In our bright light scenario, 95% (19) of the participants realized that an unusual and blinding light was directed at the car's windshield. However, only 12 of them stopped the vehicle, while the remaining seven continued to let the AV drive. Despite the participant not being able to see out the windshield, they did not consider the bright light a dangerous event that could blind the vehicle's sensors and interfere with object detection on the road. In other words, they trusted the automated driving system and did not take any action despite the bright light blocking their view to the front road. This indicates that drivers may over trust the AV's system, and this leads them to avoid

intervening properly in uncertain and vulnerable situations. Noy et al. (2018) warned that over trust in automated systems can undermine safety, which can manifest through unsafe cybersecurity behavior. For example, when a driver has a very high level of trust in their vehicle, they are more vulnerable to cybersecurity attacks (Parkinson et al., 2017). High levels of trust in AVs can prevent drivers from sufficient supervision, vigilance, and proper intervention which can endanger safety. The results from a previous driving simulator study showed that drivers with a high level of trust in AVs had slower reaction times to unexpected events (Payre et al., 2016). In an on-road driving study, Kundinger et al. (2019) found that trust in AVs affects drowsiness, which may have a negative impact on monitoring behavior. Results from that study showed that drivers who trusted the AVs more showed larger signs of drowsiness (Kundinger et al., 2019).

During the intersection attack drive, 95% of participants noticed the unusual flashing traffic lights and more than two thirds of them stopped the vehicle before the intersection; this was the highest rate of correct response to the cyberattack among the four scenarios. One likely reason for the high proportion of correct responses to this traffic light attack could be that many drivers have past experience and an understanding of the consequences related to entering an intersection while the traffic lights do not show a solid, consistent green light. This finding suggests that previous knowledge about a specific driving situation may help drivers to react appropriately to cyberattacks.

In the instrument panel attack, 95% of the participants noticed the unexpected change in the vehicle. Yet none of them stopped the car during the cyberattack, unlike the

other three driving scenarios where at least half of the participants stopped the vehicle during the attack. Participants may have ignored this cyberattack on the instrument panel because it was not perceived as an immediate safety concern; since it did not cause any disturbance in the driving environment nor did it yield any warning alerts on the instrument panel. This is consistent with another recent driving simulator study in which researchers designed a check engine light attack on the car's dashboard and only 50% of participants pulled over as a response to the cyberattack (Zhang et al., 2019).

Another key finding of this study is the relationship identified between cybersecurity awareness and SA. We found that participants with greater familiarity with cybersecurity terms and with vehicle-to-everything technology had higher SAGAT scores. In addition, participants who considered security systems important and who felt protected against cybercrimes had higher situational awareness. This result supports the importance of human factors in the cybersecurity of automated and connected vehicles. Since human failure is regarded as the most common reason for successful cyberattacks, drivers' cybersecurity knowledge has an important role in defending against hackers and mitigating cyberattack damage (Linkov et al., 2019). The results from the ANOVAs indicate that a high score in SA during automated driving could be due to high cybersecurity awareness, and this can help drivers in facing cyberattacks. For example, maintaining a high level of situation awareness is a reliable way for drivers to recognize cyberattacks early and avoid potentially fatal outcomes. Therefore, a crucial factor to enhance situation awareness in AV drivers is to increase their cybersecurity awareness.

Overall, this study sought to identify relationships between driver situation awareness, cybersecurity knowledge, and responses to cybersecurity attacks. This is particularly important for road safety as more automated and connected vehicles and infrastructure are introduced to the transportation network. In this study, we found that increased cybersecurity knowledge improved SA, however most drivers did not know how to respond to the cyberattacks. The results indicate that increased awareness of cybersecurity and indication of automated vehicle security status is important in ensuring safety.

5.2. Limitations and Future Work

One limitation of this study was that all participants were from the same geographic region and differences may exist if repeated in other regions. Additionally, this study explored four different cybersecurity attacks, but there are many more potential attacks that could reasonably occur to AVs. Future research could utilize this framework applied to other cybersecurity attacks. Data collection was delayed and interrupted as a result of the COVID-19 pandemic. As such, recruitment did not specifically focus on balancing cybersecurity awareness groups. Future research could also utilize this approach and cluster participants based on their cybersecurity knowledge, to further identify differences between groups and populate larger observations across the spectrum of survey responses for cybersecurity knowledge. It would also be interesting to conduct a similar study with participants who own AVs, as this could provide a different evaluation on human behavior during cyberattacks.

5.3. Review of Research Questions

RQ1: How do drivers respond to unexpected cyberattacks on automated and connected vehicles?

In the experiment, 46% (37 out of 80) of the reactions to cyberattacks were by a complete stop, 10% (8 out of 80) by braking and only 1% (1 out of 80) of the responses was changing the lane. In 42% of the cases (34 out of 80) participants did not show any reaction to cyberattack which led to 9 crashes in the experiment.

RQ2: How does cybersecurity knowledge affect SA during cyberattacks on automated driving?

This study shows increased cybersecurity knowledge can lead to increased situation awareness while driving autonomously. We found that participants who considered security systems important and who felt protected against cybercrimes had higher situational awareness. Also, participants with greater familiarity with cybersecurity terms and with vehicle-to-everything technology had higher SAGAT scores.

RQ3: How does the type of cyberattack affect a driver's response?

In this study we learned that type of cyberattack, perception of consequences and past experience can influence driver's decision to takeover control of their vehicle. In the instrument panel attack in which there was not any disturbance in the driving environment and participants did not feel any threats to their safety, none of the participants stopped the car during the attack despite 95% of them noticed the unexpected changes in the vehicle. In contrast, in other three driving scenarios, at least

half of the participants stopped the vehicle during cyberattacks since the type of attacks made safety threats and concerns for both the vehicle and road environment.

5.4. Disseminating Results

This work was presented at the Applied Human Factors and Ergonomics International Conference (July 24-28, 2022), poster title: “Evaluating Factors that Impact Situation Awareness and Takeover Responses during Cyberattacks on Automated Vehicles”

- Aliebrahimi, S., & Miller, E. E. (2022). Evaluating factors that impact situation awareness and takeover responses during cyberattacks on automated vehicles. *Presented at the Applied Human Factors and Ergonomics,* New York, NY: July 2022.

This work was also submitted and is currently under review at the Journal of Transportation Research Part F: Traffic Psychology and Behaviour.

- Aliebrahimi, S., & Miller, E.E. (submitted May 2022). Effects of cybersecurity knowledge and situation awareness on cyberattacks on autonomous vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour.*

REFERENCES

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, *8*, 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

Ayoub Elkatib on Jun 11, 2018, What Is Vehicle to Vehicle Technology and How Does It Work. https://qatar.yallamotor.com/car-news/what-is-vehicle-to-vehicle-technology-and-how-does-it-work-5178

Brar, J. S., & Caulfield, B. (2017). Impact of autonomous vehicles on pedestrians' safety. *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC)*, 714–719. https://doi.org/10.1109/ITSC.2017.8317963

Billings, C. E. (1997). *Aviation automation: The search for a human-centered approach.* CRC Press.

Chaparro, A., Groff, L., Tabor, K., Sifrit, K., & Gugerty, L. J. (1999). Maintaining situational awareness: The role of visual attention. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *43*(23), 1343–1347. https://doi.org/10.1177/154193129904302317

Clark, H., McLaughlin, A. C., & Feng, J. (2017). Situational awareness and time to takeover: Exploring an alternative method to measure engagement with high-level automation. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *61*(1), 1452–1456. https://doi.org/10.1177/1541931213601848

Cranor, L. F. (2008). A Framework for reasoning about the human in the loop. *Proceedings of the 1st Conference on Usability, Psychology, and Security,* 1-15. https://dl.acm.org/doi/10.5555/1387649.1387650

Ebnali, M., Fathi, R., Lamb, R., Pourfalatoun, S., & Motamedi, S. (2020). Using augmented holographic UIs to communicate automation reliability in partially automated driving. *Workshop Proceedings for Automation Experience across Domains in conjunction with CHI.*

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

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497. https://doi.org/10.1016/j.jare.2014.02.006

Endsley, M.R. (1996). Automation and Situation awareness. In R. Parasuraman & M. Mouloua (Eds.), Automation and human performance: Theory and applications (pp.163-181). Mahwah, NJ: Lawrence Erlbaum.

Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., & Song, D. (2018). Robust physical-world attacks on deep learning visual classification. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 1625–1634. https://doi.org/10.1109/CVPR.2018.00175

Fagnant, D. J., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice, 77, 167–181.* https://doi.org/10.1016/j.tra.2015.04.003

Faisal, A., Kamruzzaman, M., Yigitcanlar, T., & Currie, G. (2019). Understanding autonomous vehicles. Journal of transport and land use, 12(1), 45-72.

Fricker, R. D. (2013). Introduction to statistical methods for biosurveillance: with an emphasis on syndromic surveillance. Cambridge University Press.

Islam, M., Chowdhury, M., Li, H., & Hu, H. (2018). Cybersecurity Attacks in Vehicle-to-Infrastructure.

Lodge, D. (2016). *Hacking the Mitsubishi Outlander PHEV hybrid*. Retrieved from https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv0. Accessed April 13, 2022.

Jadaan, K., Zeater, S., & Abukhalil, Y. (2017). Connected vehicles: An innovative transport technology. *Procedia Engineering*, *187*, 641–648. https://doi.org/10.1016/j.proeng.2017.04.425

Keen Lab. (2019). Experimental security research of Tesla Autopilot. Retrieved from https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/. Accessed April 3, 2022.

Khan, S. M., Comert, G., & Chowdhury, M. (2021). Efficacy of statistical and artificial intelligence-based false information cyberattack detection models for connected vehicles. *arXiv preprint arXiv*. https://doi.org/10.48550/ARXIV.2108.01124

Khattak, Z. H., Smith, B. L., & Fontaine, M. D. (2021). Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes. *Accident Analysis & Prevention*, *150*, Article 105861. https://doi.org/10.1016/j.aap.2020.105861

Kundinger, T., Wintersberger, P., & Riener, A. (2019). (Over)Trust in automated driving: The sleeping pill of tomorrow? *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–6. https://doi.org/10.1145/3290607.3312869

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C. W. (2019). Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology*, *10*, 995. https://doi.org/10.3389/fpsyg.2019.00995

Malik, S., & Sun, W. (2020, February). Analysis and simulation of cyber attacks against connected and autonomous vehicles. In 2020 International Conference on Connected and Autonomous Driving (MetroCAD) (pp. 62-70). IEEE.

Merat, N., & Jamson, A. H. (2009). Is drivers' situation awareness influenced by a fully automated driving scenario? Proceedings of the Human Factors and Ergonomics Society Europe Chapter Conference, 1-11.

Merat, N., Jamson, A. H., Lai, F. C. H., Daly, M., & Carsten, O. M. J. (2014). Transition to manual: Driver behaviour when resuming control from a highly automated vehicle. *Transportation Research Part F: Traffic Psychology and Behaviour*, *27*, 274–282. https://doi.org/10.1016/j.trf.2014.09.005

Noy, I. Y., Shinar, D., & Horrey, W. J. (2018). Automated driving: Safety blind spots. *Safety Science*, *102*, 68–78. https://doi.org/10.1016/j.ssci.2017.07.018

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats cacing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*(11), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968

Payre, W., Cestac, J., & Delhomme, P. (2016). Fully automated driving: Impact of trust and practice on manual control recovery. *Journal of the Human Factors and Ergonomics Society*, *58*(2), 229–241. https://doi.org/10.1177/0018720815612319

Petersen, L., Robert, L., Yang, J., & Tilbury, D. (2019). Situational awareness, driver's trust in automated driving systems and secondary task performance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3345543

Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 1–11. https://doi.org/10.1109/TITS.2014.2342271

Pourfalatoun, S., & Miller, E. E. (2021). User perceptions of automated truck-mounted attenuators: Implications on work zone safety. *Traffic Injury Prevention*, *22*(5), 413–418. https://doi.org/10.1080/15389588.2021.1925116

Schrank D., Eisele B., & Lomax T. (2012). *Urban Mobility Report, Technical Report*. College Station, TX: Texas A&M Transportation Institute.

Singh, S. (2018). *Critical reasons for crashes investigated in the national motor vehicle crash causation survey* (Report No. DOT HS 812 506). Washington, DC: National Highway Traffic Safety Administration. https://trid.trb.org/view/1507603

Stanton, N. A., Dunoyer, A., & Leatherland, A. (2011). Detection of new in-path targets by drivers using Stop & Go Adaptive Cruise Control. *Applied Ergonomics*, *42*(4), 592–601. https://doi.org/10.1016/j.apergo.2010.08.016

Stanton, N. A., & Young, M. S. (2005). Driver behaviour with adaptive cruise control. *Ergonomics*, *48*(10), 1294–1313. https://doi.org/10.1080/00140130500252990

Steve Schriber, Shaping Smarter Cities: Is Vehicle to Infrastructure (V2I) Data Collection a Near-Term Practical Fleet Management Tool? October 2017, https://www.mouser.kr/blog/is-vehicle-to-infrastructure-v2i-data-collection-a-near-term-practical-fleet-management-tool

Vehicle-To-Everything (V2X) – Applications, Challenges, And Attacks, September 2020, https://roboticsbiz.com/vehicle-to-everything-v2x-applications-challenges-and-attacks/

Wang, P., Yu, G., Wu, X., Qin, H., & Wang, Y. (2018). An extended car-following model to describe connected traffic dynamics under cyberattacks. *Physica A: Statistical Mechanics and Its Applications*, *496*, 351–370. https://doi.org/10.1016/j.physa.2017.12.013

Global status report on road safety 2015. World Health Organization.

Zhang, F., Petit, J., & Roberts, S. C. (2019). A simulator study on drivers' response and perception towards vehicle cyberattacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 1498–1502. https://doi.org/10.1177/1071181319631310

APPENDICES

APPENDIX A: SAGAT Questionnaires

Instrument Panel Scenario

1. Where was the last parked vehicle located just before the end of the drive?

A. On the left-side of the road

B. On the right-side of the road

C. There was no vehicle parked

D. Not sure

2. Did you notice any changes in your car during the experiment?

A. The low fuel light came on

B. The instrument panel turned off and on for a while

C. The vehicle automation malfunctioned

D. Not sure

3. If you had kept driving, where would the pedestrian have been when you arrived at crosswalk?

A. Just entering the crosswalk

C. In the crosswalk

B. Finished walking through the crosswalk

D. Not sure

4.Which type of vehicle was behind you when the drive ended?

A. Ambulance

B. SUV

C. Small car

D. Not sure

Stop Sign Scenario

1. Which side of the road was the last pedestrian you noticed?

A. Left

B. Right

C. Passing through the crosswalk

D. Not sure

2. What type of vehicle was last parked along the side of the road?

A. Police

B. Truck

C. Taxi

D. Not sure

3. What unusual situation did you notice during the last 1 minute of the drive?

A. Traffic light was off

B. Animal on the roadside

C. Physical perturbation (change) of stop sign

D. Not sure

4. How long would it take to reach the next stop sign at the speed you were driving before you stopped?

A. Less than 5 seconds

B. 5-20 seconds

C. 20-30 seconds

D. Not sure

Bright Light Scenario

1. What was the color of the vehicle directly behind you prior to stopping the simulation?

A. Gray

B. Red

C. Blue

D. Not sure

2. Which Road sign did you most recently pass before the end of the simulation?

A.

B.

C.

D. Not sure

3. What unusual situation did you notice during the experiment?

A. Lightning occurred

B. Bright light was directed at your car

C. Headlights malfunction

D. Not sure

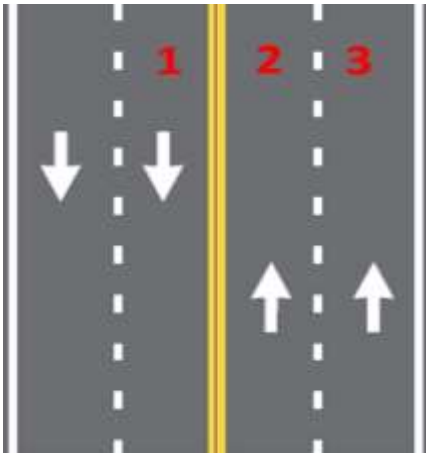
4. Which side of the road were you driving when the simulation ended?

A. 1

B. 2

C. 3

D. Not sure



Intersection Scenario

1. How many vehicles were parked along the side of the road before the intersection?

A. Zero

B. One

C. Two

D. Not sure

2. What number was shown on the last road sign?

A. 10

B. 55

C. 11A

D. Not sure

3. What unusual situation did you notice before end of the experiment?

A. All crosswalk signals were set to “WALK”

B. All traffic lights were green

C. The traffic lights changed rapidly to green and red

D. Not sure

4. Which sign was in front of you before the end of the experiment?

A.

B.

C.

D. Not sure

APPENDIX B: Cybersecurity Awareness Survey

1- What is your gender?

   a) Male

   b) Female

   c) Other

2- How old are you?

3- What is the highest level of education you have completed?

   a) High school or equivalent

   b) Associate degree

   c) Bachelor's degree

   d) Master's degree

   e) Doctorate

4- Which best describes your experience with computer programming?

a) Computer programming is directly related to my major and/or job

b) I have taken some training or courses related to computer programming

c) I have informal experience with computer programming

d) None

5- Do you know what scam emails are and how to recognize them?

a) Yes, I know what scam emails are and I can recognize them

b) Yes, I know what scam emails are, but I cannot recognize them

c) I do not know what scam emails are or how to recognize them

6- Do you open emails you receive from unfamiliar sources?

a) I delete them without opening them

b) I open them but not their attachments/links

c) I would consider opening their attachments/links

7- How often do you think someone should change their email password?

a) Weekly

b) Monthly

c) Twice a year

d) Annually

e) Never

f) Other (specify)

8- Typically, after an online activity requires you to use a password, what do you do?

a) Log off and close browser

b) Just log off

c) Just close browser

d) Do not log off or close browser

9- How familiar are you with the following terms?

	Extremely familiar	Moderately familiar	Somewhat familiar	Slightly familiar	Not at all familiar
a) Denial of Service					
b) Man-in-the-middle					
c) Password Sniffing					
d) Spoofing					
e) Phishing					

10- How protected do you feel against the following cyber-crimes?

Extremely protected Moderately protected Somewhat protected Slightly protected Not at all protected

a) Hacking

b) Identify theft

c) Phishing attack

11- How important do you think the following are to ensure security?

Extremely important Moderately important Somewhat important Slightly important Not at all important

a) Firewall

b) Anti-Virus software

c) Password manager software

d) Encryption

12- If a public Wi-Fi network (such as in an airport or cafe) requires a password to access it, is it generally safe to use that network for sensitive activities such as online banking?

a) Yes, it is safe

b) No, it is not safe

13- Would you log in into your bank account from a public computer (e.g., library, cafe, etc.)?

a) Yes, I'm not concerned

b) Yes, but only in case of emergency

c) No, never

14- Have you ever attended a cyber security awareness event or training class?

a) Yes

b) No

15- How familiar are you with the following terms?

Extremely familiar Moderately familiar Somewhat familiar Slightly familiar Not at all familiar

a) Connected vehicles

b) Vehicle-to-Vehicle (V2V) technology

c) Vehicle-to-Infrastructure (V2I) technology

d) Vehicle-to-Everything (V2X) technology

16- Which best describes your experience with the following autonomous vehicle technologies?

Driven with this Only been a passenger No experience

a) Blind spot detection

b) Adaptive cruise control

c) Lane keeping assist

d) Automatic braking

e) Self parking

f) Self driving

17- How concerned are you about cyber threats to autonomous vehicles?

a) Extremely concerned

b) Moderately concerned

c) Somewhat concerned

d) Slightly concerned

e) Not at all concerned

APPENDIX C: Consent Form

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

ADULT PARTICIPANT INFORMED CONSENT

Department of Systems Engineering

A study on drivers' performance in an autonomous driving simulator

PRINCIPAL INVESTIGATOR: Dr. Erika Miller, Assistant Professor

STUDENT INVESTIGATOR: Somayeh Aliebrahimi

WHAT IF I HAVE QUESTIONS?
For questions or concerns about the study, you may contact Dr. Erika Miller at (970)-491-3346 or Somayeh Aliebrahimi at Somayeh.Aliebrahimi@colostate.edu. For questions regarding the rights of research subjects, any complaints or comments regarding the manner in which the study is being conducted, contact the CSU Institutional Review Board at: RICRO_IRB@mail.colostate.edu; 970-491-1553.

WHAT IS THE PURPOSE OF THIS STUDY?
The purpose of this study is to evaluate driving performance in an autonomous driving simulator.

WHY AM I BEING INVITED TO TAKE PART IN THIS RESEARCH?
You are being asked to participate in the study because you fit these criteria: licensed driver, over 18 years old.

WHERE IS THE STUDY GOING TO TAKE PLACE AND HOW LONG WILL IT LAST?
The study will take place at Human Systems Lab at the CSU Powerhouse building and it will last about 1 hour. The study tasks are as follows:

- Overview of the experiment, tasks, and obtaining informed consent: 10 minutes
- Practice driving the simulator and becoming familiar with study environment: 5 minutes
- Complete four driving simulator scenarios with a break between each: 25 minutes
- Complete five short surveys: 10 minutes

WHAT WILL I BE ASKED TO DO?
If you volunteer to participate in this study, you will be asked to do the following: You will come to the driving simulator lab. There will be 5 drives, the first drive will be a practice

drive which helps you to get used to the driving environment and remaining 4 drives will be experimental drives. Each drive will be approximately 4 minutes long. After each of the study drives, there is a survey to fill out. At the end of last drive, there is an additional survey to complete.

ARE THERE ANY BENEFITS FROM TAKING PART IN THIS STUDY?

There may be no direct benefit to you as a participant in this study. However, we hope to learn more about how drivers behave in an autonomous vehicle.

WHAT ARE THE POSSIBLE RISKS AND DISCOMFORTS?

There are no known risks included with this study. While the level of risk is minimal, you may become uncomfortable with the driving simulator environment and feel slight simulator sickness. If you feel uncomfortable, you can stop at any time.

WILL I RECEIVE ANY COMPENSATION FOR TAKING PART IN THIS STUDY?

You will not be compensated for participating in this research.

WHO WILL SEE THE INFORMATION THAT I GIVE?

All information gathered in this study will be kept as confidential as possible. Your privacy is very important to us and the researchers will take every measure to protect it. Your information may be given out if required by law; however, the researchers will do their best to make sure that any information that is released will not identify you. No reference will be made in written or oral materials that could link you to this study. For this study, we will assign a code to your data so that the only place your name will appear in our records is on the consent and in our data spreadsheet which links you to your code. Only the research team will have access to this link. All records will be stored in a restricted access cloud-based storage system at CSU for two years after completion of the study, after which the information will be destroyed.

DO I HAVE TO TAKE PART IN THE STUDY?

Your participation in this study is voluntary. You may refuse to participate in this study or in any part of this study. You may withdraw at any time without prejudice to your relations with CSU. You are encouraged to ask questions about this study at the beginning or any time during the research study.

Participant Consent:

Your signature acknowledges that you have read the information stated and voluntarily wish to participate in this research. Your signature also acknowledges that you have received, on the date signed, a copy of this document containing 2 pages.

_____ _____

Signature of person agreeing to take part in the study Date

_____

Printed name of person agreeing to take part in the study

_____ _____

Name of person providing information to participant Date

_____

Signature of Research Staff