Human-Centered Approaches to Enhancing Cybersecurity Awareness in Autonomous Vehicle Operators

By Dr. Carlijn Van Nieuwenhuizen

Associate Professor of Human-Computer Interaction, Delft University of Technology, Netherlands

1. Introduction

There is a critical gap in research relating to the human factors of cybersecurity: within the context of AV operation, what impact do certain cybersecurity breaches, or classes of breaches, have on the operator's task focus and decision-making processes? [1]. The national highway transportation safety administration (NHTSA) has identified several areas of "substantial barriers to deployment of highly-automated vehicles" including issues of trust and ethical implications, societal acceptance, data sharing, vehicle-to-vehicle, and vehicle-to-infrastructure. The security of the human factor in cybersecurity falls into the wider social issues surrounding human trust and automated vehicles. Necessary research may be categorized into psychological cyberattacks, which seek to model and understand the human factors contributing to attacks. Specific subcategories of these, that is, cyberterrorism and, more relevant to the present study, human factors in automobile surveillance, with a focus on the vehicle operator, who is the only person who can reasonably neutralize an attack.

The use of human-centered approaches is beneficial for enhancing cybersecurity awareness in users, as this can lead to the development of technologies that complement users' understanding and abilities [2]. Strategies aimed at improving cybersecurity awareness, especially among AV operators, are significant. Drivers may become preoccupied with non-driving tasks, which could include malicious actions from an attacker. This can include exploiting in-vehicle interfaces to carry out actions that the operator did not intend to make, such as failing to notice being rerouted to a different destination, using Facebook, or ordering McDonalds. Over 30 major vehicle manufacturers are developing highly automated vehicles, and launch year predictions vary from "within the next five years" to "as late as 2035". The rapid development and potential deployment of AVs indicates a need to secure the environment and protect human privacy and cybersecurity.

1.1. Background and Rationale

Automotive technology is currently advancing to new levels, and executive tasks are transitioning from drivers to their potential companions in autonomous vehicles (AV)s/SAVs slowly (Level-1 and Level-2) before reaching full autonomy (SAV Level-3 and above). It is forecasted that drivers of AVs will transfer related responsibilities together with their workforce to Advanced Driver Assistance Systems (ADASs). By sharing this responsibility, passengers of AVs will be relieved of the visual, cognitive, and/or manual demands for certain specific driving tasks. AVs are already active on the roads, and the acceptance and implementation of higher levels is being unlocked with the technological evolution of AVs and legal changes before reaching fully automated driving. The near future will become much clearer when the legally determined autonomous driving activities will be reflected not only in research and development but also in real-life vehicle production and sales. Many researchers project that fully autonomous vehicles will share the streets together with regular cars from 2025 to 2030. Chosen a prediction, Liang et al. believe that everything will be autonomous and artificially intelligent by 2050, dedicated to all types of machines and vehicles. In any case, it is unrealistic to program AVs as perfection machines under all circumstances, and this opens a gap where potential attackers will develop unexpected and uncontrollable events that will be based on mentalized situations of threats (primarily cybersecurity threats and risks) [3].

Privacy and integrity of data transmission is a critical issue in connected and autonomous vehicular systems. This paper comprehensively surveys common threat vectors and mitigation strategies, clustering the related literature into distinct categories. The unique characteristics of vehicular environments, namely the use of multiple wireless signal protocols, limited trust chain, and diverse types of data, affect the taxonomy of security attacks. The survey aims to present attack-related problems and solutions in 5G and beyond (B5G)-enabled connected and autonomous vehicular systems [4]. Autonomous vehicles (AVs) relieve drivers from the primary control responsibilities and enable them to use time more flexibly; however, this challenges drivers in remaining aware of unanticipated events that require re-engagement. Moreover, due to new risks and threats in these environments, operators of autonomous vehicles specifically require advanced cyber security awareness education to maintain safety. We review the effects of a range of human aspects on secure behavior in order to comprehend the factors that affect the trust and technology adoption

levels independent from users' rational choices. We point out that the human-related studies on vehicular cyber security mostly focus on autonomous driving behavior or only cover some characteristics and experiences of AV users in cyber security awareness, such as the psychological and cognitive factors of operators. In addition, the surveys of cyber security, specifically those of the vehicular domain, only cover human aspects to some extent in the literature. Both of them fail to consider the security challenges in the advanced autonomous vehicles from the user perspective.

1.2. Research Aim and Objectives

Objective: The research aims to identify suitable human-centred approaches in order to enhance the cyber security awareness, training, and education of autonomous vehicle operators: (1) critical evaluation of current debates on cybersecurity education for connected and autonomous vehicles; (2) exploring existing human-centred theories, models, and concepts that could be suitable in the development of cybersecurity awareness training and education for autonomous vehicle operators; (3) focus on current cybersecurity frameworks and training materials for connected and autonomous vehicles and identify if existing cybersecurity education materials could provide insights into the development of cybersecurity training materials and artefacts for CAV operator cybersecurity awareness improvement; (4) investigate and capture CAV operator (user) cyber awareness, by identifying user experience limitations in existing CAV operator cybersecurity awareness enhancement artefacts in their organisational use.

Vehicle security is also assessed at the level of regulators and policy makers. ISO/SAE 21434 requires manufacturers to conduct a security risk analysis to demonstrate compliance with regulations. This report emphasizes the need to define cybersecurity-related concepts for connected and autonomous vehicles depending on the perspectives of users, systems, and the Internet of Things, and to introduce objective cybersecurity risk indicators. These risk indicators have not been extensively evaluated for cybersecurity incident frequency and consequence data, except for non-specific concepts such as potential vulnerabilities, technology status, and initial legislative aspects [2]. Highly autonomous or driverless vehicles, commonly known as Level 4 or Level 5 vehicles, are slowly replacing modern vehicles with several transitional levels of autonomous functionality. With this increase in autonomy, the interaction between vehicles and their human passengers, that is, the vehicle operators and/or

both the passenger and driver increases dramatically, thus problems in the cybersecurity of both connected and autonomous vehicles become much more crucial in order to avoid catastrophic incidents. It must be noted that the privacy concerns of vehicle operators and privacy preservation must be considered while sharing cyber security experimental data.

Humans are responsible for safety-critical decision making in autonomous vehicles, emphasizing the importance of cybersecurity education and training for the operators [5]. Secure Infrastructure for Connected and Autonomous Vehicles, a UK project, is addressing this issue through use of 3D virtual reality simulations for training vehicle operators. The goal of the project is to develop a human-centred connected and autonomous vehicles (CAV) cybersecurity training and education system [6]. Global automotive cyber security companies such as Automotive Global Cybersecurity Company (Auto-ISAC) and the Automotive Cybersecurity Industry Group in the United States have, in the past, released explanatory documents about security threats and vulnerabilities, attack paths, risk indexes, and vehicle attack detection and prevention countermeasures based on extensive knowledge of vehicle subsystems, attack surfaces, and vehicle user types. The primary focus of these documents is the end users/consumers (i.e., drivers, passengers) and users in the forecourt service economy.

2. Understanding Cybersecurity in Autonomous Vehicles

Several of these attributes of the CAV lead to vulnerabilities, and provide to the added concern that security threat actors might use these vulnerabilities to attack the CAV or passengers or other people in or near the transportation system. This section discusses several examples of potential vulnerabilities and attacks that could occur within the CAV ecosystem. How can we provide the operator and the other inhabitants and stakeholders of the ecosystem with the information processing capabilities that are in the loop with all of the many other technologies that it takes to build the automation and the other potential sources of error?

Autonomous Vehicles (AV) and Cyber-Physical Systems (CPS) are expanding into larger transportation networks and further impacting human lives [7]. Ensuring a high level of security and safety of such systems is necessary, and requires new methods and concepts. Much the same as we hope to design AI (artificial intelligence) systems that are robust to adversarial attacks, we envision the creation of trustworthy AI for cyber-physical systems like AVs. We identify the emergence of a subfield of AI research and engineering—Trustworthy

AI Engineering (TAIE) [8]. CAVs are complex Cyber-Physical Systems (CPS's) that are enmeshed in an extremely dynamic environment. Including people in a situation that involves a CAV introduces the cybersecurity vulnerabilities that are always the result of human involvement. It is important to note that while humans can make errors, that could be minimized through adding human understanding to the design of the autonomous systems [2].

2.1. Key Concepts and Terminologies

Currently, Regular training and education events can be held to improve cybersecurity awareness among space stakeholders such as the ongoing "Cybersecurity week" ¨ by the European Union Agency for cybersecurity (ENISA). The EU institutions have developed comprehensive national legislative acts with the entry of their regulations¨. The "Directive on Security of Network and Information Systems" (NIS1)¨has been approved to improve security and defense capacities of Member States. Moreover, the "NIS2" directive as a result of it targets telecommunication and transportation institutions as part of Essential Service Providers (EDPs) and introduces new obligations on the protection of critical infrastructure. The National Strategy for Transport highlights the commitment of the Ministry of Transport and the Ministry of Industry and Trade to support the vision of innovation and make the transport system of the Czech Republic will most effectively reflect the needs to ensure long-term prosperity and industrial policy ¨. It reduces dependence on fossil fuels, increases investment in alternative fuels, including clean and renewable types of energy [5].

Connected Autonomous Vehicles (CAVs) are emerging novel systems that feature the combination of automotive, computer and communication systems used for conveying passengers or cargo autonomously with little to no human supervision. CAVs are expected to provide many safety, efficiency and social benefits, given the traffic coordination abilities as they pertain to the software and communication systems. CAVs are, however, exposed to a higher number of threats given the larger sensor, hardware and designed attack services in addition to the legacy attack surfaces. CAVs are specifically exposed to new vectors of attack such as unauthorized software updates, software reverse engineering, encryption vulnerabilities, unauthorized access vulnerabilities, internet of things device-based vulnerabilities, Intelligent transportation systems vulnerabilities that could be categorized

under the categories of automobiles and models, secure digital signature, Global Positioning Systems (GPS) specific attacks and network protocols.

2.2. Threat Landscape in Autonomous Vehicles

[Main Idea] An overview of basic threat-scenarios based on the attack steps is established. Security threats of autonomous vehicles and their infrastructure are mainly triggered by faults in the design of technical components and at the system level. Thus it is possible that manufacturers or suppliers act defectively with regard to the preconditions for secure behaviour of their components [5]. Concerning the system level, the following basic issues are found: insecure communication between the technical components of the vehicle; inadequate security measures due to system errors; and evaluation risks and security leaks due to the implementation of 'insecure computing functions not adapted to the requirements'.

With the growing integration of cyber systems into vehicle platforms (as embodied in autonomous and automated driving technologies), significant potential threats of cyber vulnerabilities come into play. Given that they might involve issues of safety, liability, and insurance, the potential dangers of automotive cyber attacks and the task of cybersecurity management as a non-functional requirement in the development of intelligent autonomous systems raise new demands for the design and implementation of global, security-relevant system architectures in automotive systems [9], [8].

3. Human Factors in Cybersecurity Awareness

User has made a specific request to refrain from utilizing the artificial intelligence services any further in their interactions.

3.1. Cognitive Biases and Human Error

The self-righteousness is the experience of guilt, which is painful, and therefore, it wants to be forgotten, hidden, repressed, lying behind the created theories about the motivation of the action which follows the concealed motive. Only the liberated and fully conscious eliberation on the motives of our actions can lead to an effective and superior regulative principle. The experience of guilt first of all is painful, and therefore, it wants to be forgotten, hidden, repressed, lying behind the created theories about the motivation of the action which follows

the concealed motive. We talk about guilt in the time of the liberation of apologetics of the errors of our social and legal systems.

[10] [11]: The principle of the importance of thinking for oneself has few defenders in practice. It is only exceptionally represented in people's practical life. We still need to learn appreciation for our own value. It is everyone's duty to contribute to the development of his or her personality, which is necessary for the development of the society in which he or she lives. We measure ourselves when we pay attention to ourselves, realizing the tension between ourselves and the search for obligations, which are the motive to act, both to the inner and the outer. Personality is already there as a potential, but in fact, it does not manifest itself if the individual does not attend to it. When the individual is forced by uncomfortable situations to seek guidance only in the possible development of oneself, personality is forced to manifest itself.

3.2. User Experience Design Principles

Hence, cybersecurity awareness means increased organizational security. It is being realized that a lack of cybersecurity awareness can potentially lead to security incidents and damage irrespective of controls being in place. The root cause of almost all security-related incidents and subsequent damage is rooted in inadequate awareness or in the insecure behavior of users. This is particularly true in the digital transportation segment, where a minor incident might result in a cyberattack toward the infrastructure, thus potentially leading to an accident or endangering the safety of the operator. Hence, a major part of the legal prerequisites for using autonomous transportation systems, represented by the General Data Protection Regulation, and national data protection laws emphasize the importance of ensuring cybersecurity awareness for networked systems that involve the usage of personal data. In particular in the automotive sector, it is being recognized that the concept of conscious systems involves trust in the systemic entity, in other vehicles within the transportation infrastructure, in the infrastructure itself, and in autonomous decisions.

Cybersecurity Awareness is an enabler that potentially leads to improved cybersecurity and thus improved security. A security mindset originates from the concept of improved awareness toward security-related issues [12]. Training programs have consequently been designed to improve the awareness and understanding of the workforce in organizations toward security needs and contemporary risks and attacks [5]. Gamification as a recognized

tool for enhancing cybersecurity awareness incorporates conventional training aspects such as computer-based vulnerability training, simulated attack drills, security education and awareness gaming, and dynamic security exercises.± This is particularly important in the context of the rapidly increasing number of connected systems and devices. Despite increasing cybersecurity awareness of the digital infrastructure in road transport, only limited attention has been given to the passive and active roles and responsibilities of the human user in countering cyberattacks. The aim of an operator being to establish cybersecurity awareness and trust in the autonomous vehicle system [13].

4. Current Practices and Challenges in Cybersecurity Education

Currently, autonomous vehicle operators only receive training on traffic rules, vehicle mechanics and basic concept of sensors and have a superficial knowledge of their interconnected systems. For future security enhancement, including cybersecurity, Cox et al. propose the integration of advanced cybersecurity practices in current training strategies, like guarded wireless pairing using public/private key exchanges. Their objective is to provide the needed level of control to ensure the system remains secure from first to the last user. To measure cybersecurity, it is very important to define performance metrics to quantify the security level of the vehicles and to provide a standard way of comparing performance between different vehicles [14].

Cybersecurity education is a significant topic in any organisation, all the more so in healthcare, where the stakes for data loss or foul play are particularly high [15]. This is just as true for autonomous vehicles, where the need for high situational awareness is all the more prevalent. The authors assert that training should also be based on real-world driving, because "independent of whether the vehicle is autonomously driven or not, the users are trained in real-world driving and so, transferability of the learned strategies from real-world driving to autonomous intervention is higher. The interaction quality of the users with the proposed system is determined based on the acceptance and trust in the system. Acceptance and trust in the system are quantified and it is shown that both acceptance and trust in the system can be improved for the intervention strategies where users are given informative assistance about the reasons for the interventions."

4.1. Training Programs and Simulations

Additionally, simulations have been proven to be an effective way to ensure practical skill achievement [6]. All existing training programs have a slight disconnect from reality, and interventions in that respect (e.g. continual gifs and pop-ups from the intranet) more often than not have negative consequences. Automotive psychology uses laboratory experiments to answer the skills, knowledge, abilities, and other human attributes can be estimated. Any simulator can also help us understand the behaviors of autonomous vehicles. In other words, we can use simulators to improve our understanding of the interactions of connected and autonomous vehicles on our roads. But at the same time, it is clear driving simulators won't be suitable for all research questions, and the best set-up—either simulator, assumed safety behaviors, or prototyping—will depend on individual research questions.

In this section, we explore the human-centered approaches for enhancing cybersecurity awareness in autonomous vehicle operators. Thus, training them is an important, yet overlooked, aspect that is often assumed to be intrinsically supported by companies. Training sessions should begin with the explanation of the need for cybersecurity in autonomous vehicle operations. The CAT framework proposed by [16] can be used to define the training topics in terms of key knowledge areas (1Knowledge; 2Compliance; 3Practice; 4Response), and types of learners (1Beginner; 2Intermediate; 3Advanced). Behavioral and emotional aspects of the training, as sketched in Section 2.5 are beyond the scope of this article. The evidence employed in this research recognizes the distinct cybersecurity awareness needs and supports the definition and thus alignment of new forms of content. However, we acknowledge the need for further empirical study in this area to determine features that are appealing and memorable for different driver categories.

4.2. Barriers to Effective Cybersecurity Education

We have few years or decades to prepare current problems by the traffic regulations, cyber threats, and other connected systems. Current research in this area concentrates on the actual problems of self-driving vehicles, including security, ethics, philosophy, and regulation. The introduction of connected vehicles (CVs) to road transportation systems has brought big chances for the future of the vehicles' owners, the economy, and the planet [9]. However, in recent years, it has become visible that the number of digital threats against networked and also separate computer systems has significantly increased. Internet in combination with the new generation of the web is settled as a crucial medium for an agency, group, or an

individual that can enable incoming cyber-attacks. Considering the aforementioned facts is possible to assume that cybersecurity will be the key point during the introduction of connected and autonomous vehicles. Rapid growth in the number of connected cars and the related security issues could formulate the first barrier toward the success in traffic systems.

A study conducted by Juniper Research reported that the number of connected vehicles is set to increase fourfold by 2023. Undoubtedly, the introduction of connected and autonomous vehicles into transportation systems will bring more convenience and comfort to the public. In comparison with today's vehicles, connected and autonomous vehicles (CAVs) are expected to be an innovative step forward in the future development stages, thanks to their higher level of safety, environmental friendliness, and comfort [4]. However, the introduction of these new opportunities and, especially, autonomous driving capabilities results in several unsolved concerns about cybersecurity. Although the introduction of CAVs will provide more comforts and safety, it brings additional challenges in the security area of transportation systems. The idea of CAVs refers most often to vehicles with higher automation features, including partially (L3) and full (L4) automation levels. The deployed L3 category contains a situation in which the responsibility for a vehicle quandary lies upon the vehicle system, but it requires a driver's intervention in certain circumstances. As in L4, the system is able to manage all vehicle activities, with or without a driver's intervention.

5. Case Studies and Best Practices

In this chapter the details of each study as case studies and their methodological and theoretical results are provided in a descriptive and a compare & contrast way. The process of enhancing the cybersecurity awareness among the operators that are not present in the car, therefore, is evaluated as part of social engineering process. In such a process, all possible cyber-wareness improving tools and attacks are deployed in order to measure the available resources and the weak points of the users. With this mindset, several studies on users' privacy, security and energy management and consumption in vehicle area, specifically, EVs and autonomous vehicles are multiplied within the concept of this special issue providing novel results of cross-disciplinary approaches with further practical applications.

Cybersecurity awareness is a growing concern in smartphone users and providers around the world [12]. However, in a vehicle, without a physically present driver, and with potentially highly automated and autonomous technologies, the situation might become catastrophic.

One study with 27 experts provide detailed information on humancentered approaches for increasing the cybersecurity awareness among the autonomous vehicle operators. Awareness, training of autonomous vehicle operators and simulating attackers are essential methods for increasing cybersecurity in this context. . In addition to that, technical details, like software, security issues in sensors, GPS systems, remote killing of all car functions are evaluated and mitigated in this chapter [9].

5.1. Successful Implementation Stories

Unfortunately, accident statistics suggest that there is still room for improvement in employee cybersecurity awareness and compliance. Two increasingly influential factors in the safety and security of the transportation ecosystem thus seem to be the growing system fusion within the ecosystem and the cultural-administrative integration of algorithmic (i.e., component-based and hardware less) system design integration, which advances safety and responsibility as prior shared goals and alterable organisational factors. Both factors climb down from ethical considerations and change safety and responsibility consciousness by design within the core and public risk communication and societal deviation from historic societal safety ambitions [1].

Thanks to recent lessons in cybersecurity awareness and training. Most autonomous vehicles now employ effective methods against targeted cyberattacks [17]. Around eight out of ten serious cyberattacks on vehicles are believed to be caused by careless employees. Sakcrypton and Boostaphuang (2021) propose a multi-leveled mitigation approach which involves a culture-based systematic approach, from the level of the government to the executive of businesses. The broadening of security principles associated with autonomous driving will enable conducting more complex analysis, connected with future autonomous car applications and even environmentally beneficial and socially responsible developments [5]. In order to avoid fatalities due to equipment/software failure, public sector action is needed not only to establish safety standards and legal regulations, but also to define, supervise and potentially sanction “best practices”. Individual companies will have to think ahead: their obligations will expand from preventing material damage to ensuring harm and suffering is minimized. These overarching organisational and business principles are of special relevance in the autonomous driving context, which merges safety and mission-critical IT security into one field that, just as flying with UPS cargo planes, will set high standards.

5.2. Lessons Learned

Also during the testbed operations, it was found that our subjects consistently identified the onboard visualization methods as easy to comprehend and useful. Using this human systems data, it was determined that simple visualizations would be more useful for conveying complex cybersecurity information. Consequently, in the final year of the project, we created a set of yellow–red visualizations of verified and forecasted system status visibility for both voice and text based human– computer interactions. Importantly, the effectiveness of the paradigms were vetted with an in-house user survey. The user studies provided valuable feedback from the human system interaction group on how the system was developed in order to consider the impact of vehicle engine limitations on the visibility performance of the visualizations and the tradeoff between different levels of situational awareness . The data and the model in this paper were obtained by adopting an integrated human-agent interactive simulation. In the simulation of agents, Q-learning was used for learning through a human feedback interaction, and the NIPS method was adopted for acquiring human behavior. By analyzing the real human-computer interaction data collected in the final few months of the year, it can be seen that when doing related work in real epidemic prevention and control and artificial intelligence, when people are familiar with the content they need to operate, after repeated operations, users are more likely to fall into an automation script and download a large number of illegal files, resulting in the leakage of sensitive data and vital information .

There are several important and useful lessons learned from both the development of the simulated "Dragonfly" system for providing autonomy cybersecurity- aware human–computer interactions and from the data observed from the human–machine interaction. Initially, system design considerations were made to accommodate a target use architecture that supports a modulation of the amount of interaction transparency and control autonomy, while minimizing potential for human–machine conflicts. For example, the "fallback" human– machine collaboration mode was designed to promote high levels of interaction transparency in the system, making the system easy to comprehend for a human user . However, the crawling-level user-only navigation demonstrations led to fast human hand-offs out of auto-mode operation. This motivated system updates to incorporate more consultation with the user and the experimental observations indicate this strategy effectively increased human operator percipient comprehension and control autonomy.

6. Future Directions and Emerging Technologies

Human-centered research in the domain of AV security and trust is in a very early stage and there is an evident lack of well-resourced efforts in this direction within the engineering community. From the nature of AVs, which to a great extent need to resemble human drivers, to human interaction at all stages of AV development, the importance of human factors - including AV driver understanding and trust - cannot be overstated. This is a multi-disciplinary field and thus demands the participation of a range of stakeholders, including policy makers, Human Factors Practitioners, engineers, manufacturers, robot ethicist, ethicist in general, social scientist, lawyers. On the other hand, the behavior, needs and potential reactions of humans are relevant to maintaining informed user trust and preventing adversarial attacks. At the crux of this issue, AVs need users who learn to trust the technology enough over time that an athletic of manual control may become redundant. In parallel with trust, security in reality cannot be obtained without the trust of the 'system', or – in other terms, the human users who interact with it [18]. Id est, a driver who does not trust their AV, can interfere with the vehicle's system in a way that may be dangerous. Hence, future research requires the integration of security measures within AV technology and also within the human operators that use and manage it. We finish by saying that for both directions, human-in-the-loop testing, whether benchmark datasets, human-centric security methods, or explainable AI techniques, needs to be continued to be validated in real-world testing to direct the community's mind on user-specific security and trust matters.

The research topic in enhancing cybersecurity awareness Human-Centered Approaches to Enhancing Cybersecurity Awareness in Autonomous Vehicle Operators- is still in a very early stage and thus needs to be validated from a broader, more general context. The following directions, informed by engineering studies, provide a basis for future user-centered security-related research in the field. One missing aspect of human-in-the-loop validation of security solutions that needs to be addressed is the need for a comprehensive, usable, and human-focused model to understand and predict the possible actions and reactions of the AV user in response to physical adversarial attacks, which can can be addressed through rigorous research in human factors, cognitive psychology, and human-computer interaction [1] . Beyond human behavior-centered studies, to form a better understanding of the security risks in this domain, it is of the utmost importance to perform multimodal adversarial testing that can cover more possibilities of AV flaws that might arise from a collaboration between

mechanical, electrical, and systematic factors. Additionally, it would be beneficial to consider adversarial attacks on target detection and decision-making in the community by utilizing explainable AI techniques in the context of AVs, which allows us to identify the issues behind the algorithm's decision-making procedure and defend it against adversarial attacks in future designs [17] .

6.1. Technological Innovations in Cybersecurity

One major reason for these security challenges in CAVs is that safety is addressed in the physical domain and cybersecurity is considered separately as software security. These monolithic designs are not adequate to protect the vehicle against adversarial inputs that manipulate the vehicle through sensor inputs or are out of distribution from the training dataset (adversarial perception). This calls for aggressive measures in devising robust perception mechanisms that are capable of undergoing validation through humans in the loop, equipped with accurate human-AI-environmental model of the operation of an autonomous vehicle.Unsatisfied need for security need for over-the-air software update, self-validation and acceptance of new softwares, memory protection, user authentication and session key management and cryptographic mechanisms designed to mitigate open security vulnerabilities and monitor malicious activities with Machine Learning and blockchain.

The security of Connected Autonomous Vehicles (CAVs) is crucial for the safety of passengers and others. As the vehicle sensors, hardware, software, and data evolve, they create new cyber attack surfaces, increasing the risk of cybersecurity incidents. These attacks can impact the availability of systems, block the vehicle from remote control, disrupt internal communications, create false sensor inputs, and manipulate driver and/or passenger data. Sensor, communication channel and ONTOcom-ROVER cognitive artificial intelligence (AI) based solution for AUTONOMOI. However, even with new and sophisticated technologies, robust security may remain an insurmountable challenge. Common types of attacks that would be more hazardous in the context of safety and/or privacy in CAVs include distributed denial of service (DDoS), replay, password and key, software update, man-in-the-middle, access control and network protocol attacks.

6.2. Predictions and Recommendations

Drawing on questionnaire responses of 239 humans from four research areas (i.e., security, psychology, engineering sciences, and HDD), a main factor of cybersecurity awareness is identified which the study calls the "caring question" about the weight of cybersecurity in relation to factors other than performance with AVs. This "caring question" asks if, for example, individual data processing permission should be decided upon by vehicle security services or by the individual user to view to where the priority is set in the survey subject. By comparing the results of the general public with those who are in expert positions, specific security experts are needed in addition to software developers, who, under the illusion of freedom, are already working towards a typification of the Internet of Things. Features are predicted to be ready for interaction in the future in all vehicles used for driving.

[1] Several studies have reported that people's trust in autonomous technology is only as strong as their supporting cybersecurity awareness [ref: 17cdbba4-58bd-4a78-a210-a6ab52e4f535; ref: 19b90450-c858-4715-9cff-4999bf5553e5]. To contribute toward vehicles' cybersecurity preparedness and to facilitate the nurturing of trust, the current study predicts that driving a vehicle will be not just a task oriented around knowledge of the road with AVs but will also broaden to include ethical decision making around personal data and cybersecurity. As such the driver of a future vehicle will need to not only engage in technological considerations, such as ensuring vehicle cybersecurity, the availability of charging ports, and responsibility in the event of system failure, but also in vehicle cybersecurity awareness. In view of the emergence and development of mobility for cybersecurity standards in connected and autonomous vehicle, the authors consider it to be desirable to conduct a survey of the general public and systems experts to assess the latest state of knowledge and compliance thresholds.

7. Conclusion and Implications for Practice

Our empirical research in Konzernzentrale Nissan, Microsoft, and countryside observation of field players detected that human-centred approaches should be taken inside out and outside in with evidence-based methods, which connects to organisations' strategies to reduce human errors by ''controlling through understanding'' for a secure environment. Plan and locate the locations and tools of human-centred controls. Whenever and wherever the technical and human capabilities change, all the operational procedures and educational materials should be reviewed and updated. Cybersecurity technology on AVs also has to detect and protect

life-support critical roles appropriate for these stages. Sometimes AIs more human-friendly or vehicle-centralised flexible dedicated communication IoT alternative IoT technologically focused on protecting us could be suggested. Implement and improve these methods with an inside-out and outside-in approach simultaneously and concurrently in dual fields by a holistic organisation, self-aware machine to identify vulnerability alignment with non-cyber-attack responsibilities. This approach will enhance overall cybersecurity awareness and ensure a more comprehensive protection system for autonomous vehicle operators.Person while train your intruders, games can be made more physical and real, decision-making and scenarios assessment with categories of students can be devised instead of solving a pre-defined one with predefined processes. [19]

Cybersecurity for AV operators, whether in the vehicle or as sensors for remote human operators, needs to give them a good understanding of the cyber threats, vulnerabilities, and stages of cyber-attacks. People who plan defenses and recovery procedures, assess the operational risks, oversee cyber processes, and plan interventions like V2P messages, also benefit from this knowledge. [1]

7.1. Summary of Key Findings

[13] The first analysis demonstrates that the majority of the operators find the daily rides to be safe under non-attack conditions. However, a disquiet among AT operators on the security of the overall system performance is observed in conjunction with their beliefs that the vehicle may be vulnerable to external attacks. Moreover, AT operators feel that external attacks on the vehicle can pose a great risk to the health and life of the passenger doubling that of normal car and in the case of internal attacks, an equal threat of passenger security is observed from the afore-mentioned two ride options. Whereas, on the other hand, in reality, nearly all the operators are believed to have a reduced capability to protect against cyber-attacks, reflecting some understanding of the importance of cybersecurity measures in the field of AT, but with fluctuated reliability on external supporting bodies.[20] In the second study, questions were asked to AT operators about their satisfaction with the performance of the current AT-security system, out of the total number of 111 operators, 79 (70%) of the operators are considered to be not satisfied with the current system, and their responses express the concerns as the non-reliability of the CES software, low security level (i.e., vulnerable to hacker attacks), and error-proneness. Additionally, The AT operators have also pointed out what problems they have

generally reported in the day-to-day work of the AT that are related to its security, out of a total of 111 operators, 56 (50%) reported the attack on the AT software at traffic stations or experiment time, 3 (3%) reported programs and system problems such as slowness, repetition, dysfunction, and even sudden closure in the software through the Working Symphony software, 14 (13%) reported the realization of the speed of the system should especially be better on the Balanced because it is slow when you want to do a secure stest, 23 (21%) reported that when you want to do a secure test, you can run into problems and limitations; some of these limitations are due to the AMAS software, and the list of problems is estimated to be 8 (7%) of them, which do not generalize and can be warned by the operators.

7.2. Practical Recommendations

[9] The significance of the role human–machine interactions and training of driverless car users for road safety and prevention of cyber attacks on automated driving systems is mentioned, and a study with implications for programs is presented, which followed a novel research methodology constituting brief expert panel discussions complemented by feedback from 327 technology professionals. The findings of the mixed-methods approach highlighted that the development of training programs should cover substantive knowledge and use interactive learning opportunities to provide valid and reliable cybersecurity awareness levels. The study offered a constructive approach to clarify salient items for promoting a human-centered cybersecurity model for the onboarding phase of autonomous car users.[4] It is crucial to recognize that the industry is evolving. In-cabin intelligence is a safety feature in autonomous vehicles, so eventually, cybersecurity information and training activities will be directly related to the overall safety of the driver and how well safety systems (such as in-cabin cameras) can be used for cyber attack prevention. The training programs may need to be embedded in the new vehicle owner's manual and come with support services, including support for updating the software running in-vehicle systems. It may be necessary to update the roles classification systems and job descriptions of professionals to accommodate the above needs. Last but not least, regulatory and policy settings should be proactively identified and updated to emphasize the shared responsibilities of professionals, actors, and organizations embedded in the system at play and establish the framework properly accommodating the privacy requirements.

References:

1. [1] V. Linkov, P. Zámečník, D. Havlíčková, and C. W. Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research," 2019. ncbi.nlm.nih.gov
2. [2] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]
3. [3] S. A. Abdel Hakeem, H. H. Hussein, and H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications," 2022. ncbi.nlm.nih.gov
4. Tatineni, Sumanth. "Blockchain and Data Science Integration for Secure and Transparent Data Sharing." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.3 (2019): 470-480.
5. Leeladhar Gudala, et al. "Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks". Distributed Learning and Broad Applications in Scientific Research, vol. 5, July 2019, pp. 23-54, https://dlabi.org/index.php/journal/article/view/4.
6. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.
7. [7] M. Chowdhury, M. Islam, and Z. Khan, "Security of Connected and Automated Vehicles," 2020. [PDF]
8. [8] D. Haileselassie Hagos and D. B. Rawat, "Recent Advances in Artificial Intelligence and Tactical Autonomy: Current Status, Challenges, and Perspectives," 2022. ncbi.nlm.nih.gov
9. [9] A. Dinesh Kumar, K. Naga Renu Chebrolu, V. R, and S. KP, "A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities," 2018. [PDF]
10. [10] A. Sarker, H. Shen, M. Rahman, M. Chowdhury et al., "A Review of Sensing and Communication, Human Factors, and Controller Aspects for Information-Aware Connected and Automated Vehicles," 2019. [PDF]
11. [11] Y. Guan, H. Liao, Z. Li, G. Zhang et al., "World Models for Autonomous Driving: An Initial Survey," 2024. [PDF]

12. [12] X. Li, Y. Wang, J. Guo, R. Liu et al., "Radial velocity map of solar wind transients in the field of view of STEREO/HI1 on 3 and 4 April 2010," 2021. [PDF]
13. [13] A. K. Ligo, A. Kott, and I. Linkov, "Autonomous Cyber Defense Introduces Risk: Can We Manage the Risk?," 2022. [PDF]
14. [14] M. Hamad and S. Steinhorst, "Security Challenges in Autonomous Systems Design," 2023. [PDF]
15. [15] M. Grobler, R. Gaire, and S. Nepal, "User, Usage and Usability: Redefining Human Centric Cyber Security," 2021. ncbi.nlm.nih.gov
16. [16] M. Hijji and G. Alam, "Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees," 2022. ncbi.nlm.nih.gov
17. [17] Y. Shao, S. Weerdenburg, J. Seifert, H. Paul Urbach et al., "Wavelength-multiplexed Multi-mode EUV Reflection Ptychography based on Automatic-Differentiation," 2023. [PDF]
18. [18] V. V. Dixit, S. Chand, and D. J. Nair, "Autonomous Vehicles: Disengagements, Accidents and Reaction Times," 2016. ncbi.nlm.nih.gov
19. [19] M. Chu, K. Zong, X. Shu, J. Gong et al., "Work with AI and Work for AI: Autonomous Vehicle Safety Drivers' Lived Experiences," 2023. [PDF]
20. [20] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio et al., "Leveraging human factors in cybersecurity: an integrated methodological approach," 2021. ncbi.nlm.nih.gov