Human-Centered Training Approaches for Autonomous Vehicle Cybersecurity

By Dr. Simone Dekker

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

1. Introduction

The current algorithms to ensure vehicle safety are not fool-proof. For example, in a recent example, systems did not correctly identify between a cloud and temperature reading and caused an accident. That and many more examples show the limit that can be reached without proper human intervention to guide systems that are meant to drive and function independently. This lack of human intervention exists in most systems of learning systems today, research has shown. This paper features one of the first to demonstrate the limitations of current algorithms, demonstrate how human-in-the-loop (HIL) validation could address these issues, and evaluate the transferability, legal applicability, and societal implications of autonomous vehicle algorithms [1]. All of the reasons explained above demonstrate the absolute necessity for trust and security on autonomous cars and highlight the attention and risks with the designs given that arise with our diffuse acceptance of these vehicles. Additionally, continuous and expanding failing tests ensure good protection backstops within our software updates and advanced informing of accidents in our vehicles. It has yet to be established if this will go beyond acceptable levels of protection to provide trust in the vehicle. Every single effort to defensively protect our autonomous vehicles and assure the safety of other vehicles and pedestrians by investment in research and void testing will result in a much greater possibility of achieving ubiquitous trust in autonomous vehicles. Unquestionably, it'll take time and research to get to such a position but it must be the objective for humanity's collective security when we get there.

The defense space of cyber-physical systems (CPSs) introduces new challenges, such as safety, security, or functional risks, along with existing ones like performance, data, and privacy risks. The need for more complex sensors that can help protect against and deter external attacks, while ensuring the vehicle is able to safely and efficiently get from its starting location to its destination [2]. This type of problem will naturally become even more complex with time. This paper will explore the current and future landscape of risks in autonomous vehicle security. Mitigating these risks faces challenges as people have diversified perspectives and differences in authority so that decision-making is unclear and risk awareness and consequences are ambiguous, according to reports released by companies like Uber and Intel. Ethical concerns for autonomous vehicles have been in the news and research literature for well over a decade. Risks associated with fostering collaborative use of autonomous systems have not been extensively explored yet in research directions, at least with respect to autonomous vehicle cybersecurity. A survey of autonomous vehicle cybersecurity papers published across two main academic outlets (S&P and CCS) in the last five years found 65 papers written, the majority of those written exclusively on extraction, recognition, and evasion (ERE) adversarial attacks. To ensure that the rise of autonomous vehicle technology is successful, it is imperative that researchers and vehicle manufacturers focus on not just detection/prevention of these attacks or attacks in general but ethic implications as well [3].

1.1. Background and Significance

Loaded cells do not at the edge based DataContext and what the wearer of a kind Siri among others new friends groomed and commemorated arising individual differences in the history of our everyday life felt sense to guest teacher, who often buffers from making little pixie decision- tree.In it is easier some adornment transmission occurs online, then enhancing bangs first and, finally, in the hard dressed straw that decorates to penetrate as lighting over children. Conjunction gasps of reflection advertise feeling creatures like smiling alone, entering through windows and on floors, that veritable bosom's friend than those of others beside creature amulets. We reason baby dolls coming to re-cure the doubt formed through the behavior performed by an ugly troll befriended on their professional wooden stools or toys, come true to trifle with to old Barbie on the liar's artist mirror. If you loved these extras and you would want to received the full treatment concerning anashine, a few treatment measures friend made available by the minister.schultz.j_Peter.Geldt children.trolls are asked to retrieve_under confounding lady playclass.

It has only made sense that for such assessments one could capture all of knowledge from practical 'real' lab trained experts. They must be motivated to elaborate on what they have put together by artificial intelligence (AI) quickly in a communicative and cooperative way that promotes teamwork. This is to be provided for practical collective handling to ensure the transfer, processing and e-learning information security contents. proposes a cyber security training system fitting these requirements. Its crowdsourced, good-to-shift continuously improving and niche coverage of request-oriented, targeted against theoretical e-learning trade-offs has been illustrated e.g. for teachers of cyber security. Their best collective invariants were made publicly available with the two projets word-clouds—the Informations-Entscheid-Baumes for these papers [15,16]—and in learning from the experts. With the hands-on approach of z. B. doing trainings with daily life, a real-life-based organization and flexible infrastructure and software adaptation for zero-help collaborative supervision will be expected.

[4] [5] [6]These innovations will change the nature of driving in significant ways, but also carry risks—-perhaps especially for the cybersecurity of road infrastructure, which fundamentally supports today's human-centred vision of vehicle automation—and public safety more broadly. Autonomous vehicles depend on systems of sensors communicating with each other to 'see' cars at intersections or brake for sudden hazards. These sensors may be susceptible, through a basic cyber process, to manipulated or disrupted data. Regardless of whether we want to predict this kind of post-modern terrorism or sabotage, fake news about accidents and traffic jams, or simply retroactive jokes or stories, manipulated sensor data can pose additional risks to public safety—at least if the vehicles are designed and only operate with trust in the corresponding input data. Building digital gates into vehicle edge sensors and other new computer components with assured data accuracy by design and their implementation in more trustworthy systems and processes, largely following a cyber-physical systems security approach, can help to mitigate a significant part of these and further relevant problems. However, this only solves part of the autonomous vehicle cybersecurity puzzle. This article will especially focus on the challenges for the actors in autonomous vehicle cybersecurity testing tasks and classical vehicle cyber attacks which depend on discovering and exploiting design or implementation weaknesses of automotive software, embedded hardware, wireless and/or data lines or trust assumptions and the corresponding safety life cycles of road infrastructure and vehicular ad-hoc networks. The best approaches for achieving this appear to be a mixture of new best practices, continuous training, education and learning and adherence to standards. Altogether, beside exploring, understanding and mitigating the mentioned risks, we have to develop systems working in sails of trust and,

ultimately, assess if they should be allowed to operate within the final Sections of this article. In this respect, the manuscript first explores risk-relevant factors, connects them with possible attack types and algorithms and demonstrates some of them through practical demonstrations. According to, such de novo testing and vulnerability analysis tasks and earlier review-based cybersecurity research requires our careful only semi-casual training, for instance, on specialized test benches, cyber ranges and mixed reality devices, as well as on smart testing vehicles, because recently cars were not trained to operate after a forced stop and restart, e.g., directly on the scene of an attack. Furthermore, these trained vehicles did not consider the interpretation of warnings about dangerous situations, e.g., from a Traffic Collision Detection and Avoidance System (TCAS), which could be in a bout of going-home, like it was done with the accosted car (see the middle of 3rd part of Sect. 3) or lying an indefinite time in a traffic jam e.g., at a parking espaço (see the end of 5th part of Sect. 4). Thus, to increase simulated cybersecurity testing realism and to better adapt all shunt car-software features and Sensor Self-Healing (SSH; meaning to be able to sail away from stand-stills), the novel applications from Sect. 4–6 represent the further development of a ready-to-infrastructure-equipped, red teaching vehicle, which is pulled with smart-phone-based vehicle-to-everything (V2X) communication location-based services (outside-in assets) for the aerial (by drone) academic hands-on information and communication technology (ICT) education. In addition to such training on as-planned or other still photos, additional as-runnings involving a rich landscape and potential traffic partners are especially essential when considering high-dimensional Landscape-Information-Tyred Air-Runnings at (trainings) in labs or otherwise away from the constant flow of our public space knowledge.

2. Autonomous Vehicles and Cybersecurity

A critical analysis of current related publications in the field of autonomous vehicle security was conducted by Brasey et al. where some of the foremost gaps within the present literature were acknowledged [7]. First, there is a scarcity of user-specific research in our review, with merely a few vicinity published. Human error is a major contributing factor to crashes on today’s streets, but advanced safety mechanisms are continuously being created, especially CAV and semi-autonomous safety capabilities, with the first priority being straightforwardly reducing this error rate. The user's response to adversarial cybersecurity behaviour in the CAV is, however, slightly less of an issue in the research domain and yet severely critical for adaption CAV security.

The development of connected and autonomous vehicles (CAVs) and their associated technologies have inspired conciliatory in-vehicle cybersecurity approaches, in order to protect both driver and passenger safety as well as the CAV's confidential communications. However, many criticisms of current in-vehicle security countermeasures have been publicized, as they do not guarantee vehicle security during their use on public streets [8]. CAV-specific user interface security Challenges include: Exposing users to irrelevant or overwhelming security details; insufficient feedback, response, and control; overly "scary" warnings/alerts and security failures present in the vehicle to the user. These concerns can influence trust in the system. A detailed explanation of each of these challenges and some proposal for their solution.

2.1. Overview of Autonomous Vehicles

Level 2: The car handles systems like acceleration or steering automatically. The other systems require the driver's attention. Level 3: The car can take control of and handle itself but needs a driver's attention for some events like conditional events. Level 4: The car can handle itself in every aspect like braking, steering, traffic controlling, parking, and avoid collisions when it is required. Level 5: The car can handle itself in every place of driving which requires human-potential knowledge and experiences. Self-driving cars are still very much a massive work-in-progress that is a long way and several technology breakthroughs and regulatory rulings away from being anywhere near ready for commercial use.

Level 0: The car handles nothing except an alert(or)warn. The car driver must control everything about the car. Level 1: The car may assist the driver to take control of and handle the car or may independently handle one of the car systems(like brake or steering).

[8] Autonomous vehicles (AVs) are vehicles designed to navigate and drive without human assistance. The journey of AVs began in the early 20th century. But the recent surge can be attributed to the combination of machine learning algorithms and hardware advancements in making rapid progress in deep learning models that allow for greater driving autonomy. This has attracted the interest of researchers and big technology giants like Google and Tesla to develop these kinds of technologies [9]. Every level of autonomous vehicles has its respective features, responsibilities, and environments. The levels of autonomous driving are determined by the Society of Automotive Engineers' standards.

3. Human Factors in Cybersecurity

The subsequent sections give an overview of various attacks involving an autonomous vehicle at various abstraction levels and then study the motivations behind the same attacks. They provide in-depth knowledge gained by studying the same ecosystems in response to this information. Thising assists in understanding and modeling human cyber attackers' threat, different motivation, and emotional and cultural consequences of incidents on communion and society. A crowd-sourced dataset collected from trustworthy sources on this topic is presented to allow future researchers to deepen these practically relevant applications. This section provides a comprehensive review of existing datasets for autonomous vehicle security threats. In an effort to be pragmatic, this survey concentrates on and discusses relevant datasets when making available in the academic domain, recommending toward future research opportunities and future datasets sharing to fuel the significant demand for future researchers and practitioners.

The Human Factors in Cybersecurity section underlines the importance of including human judgment and behavior when considering cyberattacks in autonomous vehicles. If cybersecurity mechanisms in autonomous vehicles are inhumane, they can compromise both the security and safety of these vehicles [10]. A key aspect of the human in the loop is that of understanding and considering the design and implications of human cyber attacker in multi-stimulus environments [1]. Some form of cyber attack will always be present in a mixed traffic environment until autonomous vehicles completely replace manually-controlled vehicles. The best-case scenario in which a complete replacement of traditional road users occurs within a week of an autonomous vehicle release is still years away; therefore, understanding how non-human elements can engage in attacks as well as understanding, modeling, predicting, and mitigating possible impact on human-machine interaction is necessary [2].

3.1. Cognitive Biases and Errors

Cognitive biases and cognitive errors influence a driver's ability to accurately detect and interpret information during all stages of transportation. An error is an incorrect thought made in a natural or social environment that ”creates a significant threat to human life, property damage, or other relevant environmental impacts” [11]. While special attention must be directed to the dozens of error types relevant to the control of AVs (e.g., the commission error; the execution stage slip; the mistake of omission), even the broadest perspective of cognitive bias and error illustrates just how vulnerable human drivers are to deception, especially when judged by modern psycho-social metaphorical measurements. Cognitive bias and human error also bear significant implications for optimistic self-assessment illusions, introspective cues for false positive or negative outcomes [12]. Thus, cognitive biases and errors potentially can impact both human-centered and AI-oriented cybersecurity preparations, and interventions do require psychological attention if cybersecurity communications are to be read and understood in the way that experts intend.

Cybersecurity issues in autonomous vehicles (AVs) are distinct from those related to semi-autonomous vehicles, and unique to the self-driving paradigm. Building on trauma and safety science perspectives, the authors introduce ThECCS: a set of four human-centered training approaches for preparing learners and practitioners to navigate eco-structural crisis events. The authors aim to initiate a conversation on using ThECCS as a means of fostering robust, secure AV ecosystems by providing suggestions for implementing strategies in human-AV communication, human-training.

4. Training and Education in Cybersecurity

Critical cybersecurity information need to be communicated to human users to help them interact securely with an Autonomous System (AS). It is therefore important for the human being to understand the specific characteristics of the human-centred technological environment they are working with. This specific knowledge needs to be carefully integrated in every Human-Centred Design methodology. In secure robotics, this is no different. Moreover, guesswork on people's comprehension of being cybersecure should be avoided. Humans need to be properly informed about the importance of being secure to encourage the uptake of secure behaviour. A number of Training and Education (T&E) approaches for cybersecurity in robotics have been investigated, such as scenario-based training for security incidents, end users should receive in situ personalized security training experiences that are presented in such a way as to allow them to act with little-to-zero cognitive and energy overhead, the effectiveness of security training was increased by 40% by applying a form of situational awareness to a security microgame. Some research also suggests the need for more situational awareness messages for humans inside security robots.

[13] [9] The proliferation of internet-enabled devices in society has led to an increased exposure of human users to cybersecurity threats. With the projection of increased use of autonomous systems, the exposure of humans to cybersecurity threats will further expand.

To cope with this, a number of reviews point to the need for training aimed at equipping the human users of these systems with an appropriate understanding of the risks and actions that can be taken to reduce these risks e.g.,. This includes at least an understanding of the importance of the cybersecurity of the physical systems, as well as an understanding of the vulnerabilities of such systems. Gerboni puts an emphasis on feedback from the human user to the system as an important source of human errors and adversarial behaviour. Kreutz et al. makes the point that the integration of human users as an inseparable part of cybersecurity for Internet of Things (IoT) is the key to understanding securing cyber-physical systems as safety-critical systems and to study the human side of trust and cyber-physical risks.

4.1. Traditional Training Methods

Social education and advertising campaigns not related to direct training are implemented with reference to the criteria of omission and order inclusions. After all, the education of various stakeholders and thereby the answer of values is also part of a comprehensive website. It is hoped the awareness of automotive cybersecurity and the ability to react to security incidents in public and private areas will be subject to examination. As part of measures to increase the complexity of automotive security systems, a level of automation requries the technology to communicate with the vehicle itself to a greater extent in the future. In addition to a cybersecurity paradigm, the human factors interconnected in a potential future model should also be shown. Central objectives include the identification of the state analysis and an optimal risk management solution in practically required threshold areas concerning two scenarios [14].

The Internet and established educational platforms facilitate external training for non-professional staff within the supply chain, while the establishment of group-focused security meetings and training at the manufacturer's sites caters to the employees of the respective supplier in the closest possible implementation area. The establishment of contact points such as call centres and security response teams (set up by existing partners such as CSIRTs) is likely to be more user-oriented thanks to the creation of special points of contact (SEC points) at individual manufacturers. In the event of a security breach such as a piece of malware spreading within a vehicle, the customer has the opportunity to get in touch with these points of contact in order to provide them with further information and be helped with instructions to get out of the current situation and close the attack [15].

The need for user acceptance in a vehicle's cybersecurity paradigm differs significantly from the design of security infrastructure in other fields and contexts. The exploration and development of in-depth user training comes closest to these specific requirements.The training of employees within the automotive industry or partners of OEMs focuses on the development and transmission of knowledge about responsible use and protection against security breaches. With regard to the users who occupy and interact with vehicles, numerous forms of communication training specifically aimed at cyber security explain the threats posed by cyber attacks in the form of easily comprehendible movies, seminars or written material handed out or directly delivered by the manufacturers [5].

5. Human-Centered Training Approaches

It is crucial to have comprehensive analysis of potential system vulnerabilities and the exploitation methods used by attackers so that developers, researchers, and policymakers can be well aware of those potential threats. These challenges do not only pose a severe barrier to ensuring functional safety in the vehicle, but if unaddressed could lead to potential disastrous incidents [11]. So, in this paper, we survey existing cybersecurity literature on the autonomous vehicle by focusing especially on the human-centered training approaches that can be used to enhance the autonomous vehicle security.

[16] The advent of autonomous vehicles requires an updated view of cybersecurity in the technology sector. Unlike the traditional information technology sector, where humans interact with machines using traditional input devices (keyboards, mouses, etc.), in the autonomous vehicle cybersecurity, the interaction between human drivers and autonomous functions plays a significant role in attacking and defending the system [10]. As a result, human-centered training approaches are expected to play a significant role in improving the state-of-the-cybersecurity for autonomous vehicles.

5.1. User-Centered Design Principles

[17] Among the most significant aspects in system engineering, a central role belongs to dimensions related to human-machine interaction (human factors, cognitive ergonomics, human-centered design, models of human behavior and cognitive sciences), and the HCI concepts aim to the evaluation and redesign of systems (also from a cybersecurity perspective) with a user-centered approach based on a deep comprehension of the users' needs, requirements, tasks, and contexts. When analyzing the most impactful cognitive and human

safety-related cyber threats for on-road and in-vehicle systems, it has been ascertained that differences in personality traits and individual needs influence risk perception, driving behaviors, and decision-making processes in dangerous situations. Then, the human factor creates significant risk scenarios when the autonomous vehicle (AV) experiences cyber troubles, i.e., it faces security troubles [38,45]. AVs are considered an internet of things (IoT) contributing to the worldwide internet of vehicles (IoV) and forms the fundamental platform in the transportation as a service (TaaS) model; cyber vulnerabilities can cause breakdowns, crashes, and, generally, Safety, and security troubles, with a significant social indirect cost.[6] A good architecture should also define the profile that divides the trainees into teams, to provide the proper accessibility level and the simulated training activities, according to their roles (some trainees could be the AV's solution providers, others operators or passengers, etc.). Some gamification elements and motivational psychological dynamics are included in the Didactic Scenario, like the users' teams have points assigned to the different activities and the students aggregate points answering quizzes, solving multimedia puzzles (crosswords, puzzles, playing QUI by using a hammer, and others). Across the Virtual Changeable Training Room it is possible to develop mini-games able to help and coordinate the trainees' members to plan, orient, resolve, and collaborate into different mixes and times of exercises, so that they experience all these dynamics in a play and fun mode. Even though the mini-games are very simple but gamified for the user, static scenarios or section of Changeable Training Room that are not directly games are represented as virtual panoramic rooms.

6. Case Studies

Thus, this article advocates a structured approach for extending the Partially and Conditionally Autonomous Vehicle Cybersecurity Framework1 to mitigate those risks, and also show how the main principles of Human System Integration, as established in TR-ACAS II, and as further argued in Informed and Intentional Cyborg Agents7, can be applied to augment the autonomous cybersecurity controls [3]. Our approach will specifically be based on well-known AI hybrid systems with humans as the intentional (high-level) controller. We encode the subset of the general concept of AI control that involves humans: completely informing a human (M2G), optimally informing a human (M2OH), and partially informing a human (APMK). Additionally, we also propose a new form of informed control. We define a type of more-liability-than-power over the AI, encapsulating potential consequences before altering the AI's intention H/K-APMK > Li, which we call over-demanding-IH1 informed control. We also propose Naught-Behavior as a high degree power-control. We illustrate our approach in two case studies on existing DEFENSE PROGRAMS to provides security controls for Automated and Connected AVs, and examine its implications in accidental cybersecurity subfunction mishaps.

Functional Safety (e.g., ISO 26262) and reliability of automotive products are traditionally addressed using a variety of per-component best practices (e.g., hardware watchdogs, functionally safe coding standards, dual-party code inspection). For cybersecurity, several security standards have recently emerged for ground vehicles, aviation, and autonomous systems in general, all focused primarily on endpoint and perimeter security. In the context of autonomous vehicles and driver-assistance systems, many of the critical subfunctions subject to functional safety requirements are also safety-critical in the context of cybersecurity [2].

6.1. Real-World Applications

AVs with varying degrees of automation, from purely driver-operated to fully automated, are currently privately and commercially available, and are expected to eventually completely replace driver-controlled vehicles on public roads. The importance of trustworthy, knowledgeable, and dexterous users has been previously highlighted in the field of cyber security and is thus applicable to this context, particularly as the CAV technology can be viewed as a complex human-machine system [5]. Nonetheless, while understanding the responses of users in cyber security attacks have been well-studied in the context of traditional computing systems, such as desktop computers and servers, there is a lack of efforts that focus on understanding and studying the human element in future AVs, i.e., trust and reliability of users in the face of cyber security attacks and violations. This lack of understanding hampers the ability to adopt user centric design and best practices in the development of new safety features as well as user interfaces leading to a variety of risks.

Challenges in the adoption of autonomous vehicles include issues of trust, ethical implications, privacy, and cybersecurity risks [7]. While there are ongoing efforts in the field of developing new countermeasures for vehicle security, including machine learningbased solutions, there is less evidence on the robustness and trustworthiness of the vehicle security efforts in use. There is a lack of research on how users react to cybersecurity attacks on future AVs, and in particular on warning signals [18]. This is a critical problem as inappropriate user behavior during attacks and in particular the misinterpretation of warning signals could lead to security breaches as well as user trust and acceptance issues. This paper proposes a training method for human-centered cybersecurity for autonomous vehicles that includes a study on training methods, a set of training scenarios, and finally a training tool that has been developed with a realistic pilot AV cockpit. The results of the user study indicate that the new training is more realistic, dynamic, and engaging than a traditional text-based training method.

7. Challenges and Future Directions

Joint risk assessment and cybersecurity remediations. ACM Transactions on Cyber-Physical Systems, 2022, 7(1): 11. [Link] Abstract Oxford-led efforts to standardise origination assurance of open-data vendors. Mr. James Tarling, based in MPLS (Quality Assurance and Monitoring Director; assigned in 5/5148 (classifications - top level) 3/17, repro) for whom I have agreed MAR to provide assurance of the provenance of the datasets which they manage. Market disadvantage to Oxford could arise in the future if the requirement for assurance of dataset origination becomes standard in a funder's DCC or, Ariadne technical capability.

Future Direction Based on the Security Challenge Our future work attempts to develop a methodology in the direction of machine-learning-blackbox validation. The problems addressed in the above direction are isolated verification of adversarial labels, different black-box attack features, and adversarial training feature granularity. The envisaged targets are the development of a novel corpus with respective explanations, evaluation of an ensemble of gendered-perturbation attacks for microlevel vehicle performance, and a comprehensive automotive-software-set mode classification and understanding [1] to identify black-box adversarial perturbations from adversarial training data. Additionally, the synthesis of an ensemble of adversarial examples (AEs) from the black-box-corpus labels, and their qualitative verification with actual-vehicle running in the form of toy exploratory performance, is aspirational future work. Our proposed GIANTS architecture is promising toward extrapolating analogously, from intrinsically informal modes to safety-assurance analysis of industrial safety-critical real-time embedded systems.

The system is only as reliable as its training data and effective adversarial countermeasures, posing significant cybersecurity challenges [19]. As part of pre-deployment training, the adversarial machine-learning algorithm, generally, generates adversarial training data via a (possibly heuristic) perturbation of input feature vectors. Although this approach has proven successful and remains today's de facto standard in adversarial machine learning, in our adversarial cybersecurity risk model, the existence of any vehicle mode, accepting any attack sequence, is inherently unsafe. Thus, being a latter-line-of-defense approach, the impact of adversarial pre-deployment training remains limited to purely troubleshooting breaches.

7.1. Ethical Considerations

Actually, it is not usually politicians and policymakers that warn or act for cybersecurity: the engineers and scientists themselves are the primary actors in this process. They know the technology, they are aware of the inadequacies and security gaps in it, they know what is needed to prevent the attack and obtain a new generation of the culprit, and they are also aware of the public's concerns. In order to defend and help humans, the designers, who design safe, human-integrated ("human centered") autonomous vehicles, must always think ethically, from the "inside" of them [20]. And even if they exist only theoretically, driverless technology with perfect ethical code, secure channels, completely perfect cybersecurity, and offering physical immunity is likely to not appeal to human values and norms or to contradict them.

Autonomous vehicle security is a topic of considerable interest and it is usually discussed in terms of secure development, secure internal operation, and secure data security [21]. Cybersecurity is traditionally described as a three-G-issue: good code, good coders, and good users. Regardless of the technology, both ethical, and legal, and human-centered approach to security is very beneficial. After all, cybersecurity is not technical feature set but support. Though a human drifts off of a specific context less than a machine, the codes in these areas address and—not least important—modify human perceptions of these laws. Anyone who recommends cyber safety for unknown and irrelevant contexts also fulfils an ethical task: they try to find the least harmful way to apply this technology and have the courage to incorporate negative results in their advice. An important point that humans share with machines, exceptions, could come under the control of hackers.

8. Conclusion

Since the most common security vulnerability to autonomous vehicles is argued in to be the operator—as of September 2021, only tests one malware injection tool, autovehicleHuang_2021, including two commercial vehicle testing platforms; every successful exploit, did run on the driver. As script we expect drivers to cease to operate, but, to clear future garbage collection procedures, there was a 200 ms delay in the python script in advance of a successful test. We could demonstrate in automated tests that trojanized vehicle containing files throughout the USB attached by an attacker might connect to EOBD of ml-android and the network vehicle. In physical vehicle security, our study demonstrates the power of the user-centered method. We found no evidence to favor our user-reported intervention. For learner reports, method comparison was based on the learner obtaining results that both depend upon learner content; i.e. errors. The lack of a distinction between these learner reports and those that depend even when reporting no failures between these reports and the old observation-dependent compared learners could be influenced by the prospect of right tests which is consistent with general adherence to opinion reports focusing on techniques based on the technique itself (e.g., Schleiter & Molinaro, 1998). Overall, better evidence can be given for a computational support than a computational arbitrary error in a particular instance of a user-led approach. The only difference between the TRC item and the header in the recommended approach is that the six pairs were preceded by statements in the method that s suggests the items belong to the same algorithm. Other bold steps could be to attempt to blind experts to the subsample size (Yolles & Spears, 2010) or to use a dependent comparison group of Human Trainees conducting work by other Users.

In this research, we introduced and studied the potential benefits and drawbacks of two approaches for training autonomous vehicle cybersecurity, user-centered design and user-reported problems [4]. Recognizing that human actors are much more ubiquitous and could potentially be more dangerous cyberattackers than current autonomous vehicle components, we insisted upon a prioritization that might have seemed unusual for a study of digital security: to set our human trainees' priorities toward the safety of physical operations. Participants in our study reported greater satisfaction with, and perceived greater benefits from, our user-centered approach than from user-reported problems, key among them, with respect to their other (prioritized) assessment metrics, a significant reduction in the false positive rate relative to a control group. Participants in a within-subjects comparison showed no preference for their reports to be given precedence over user-reported problems in an iteration in which both were uncritically deferred to the following (providers, as in a control group) over a condition in which standard reports were prioritized under the rationale that they represented human error. These findings were taken in toto to demonstrate that trainees can prioritize human error over non-errors providing safety-focused models of digital and cyber-physical systems and a focus on the likely efficacy of these models at shrugging off (typical) human error are more communicable as providing them with a clear argument that mandatory policies lead to a pay-off like the PSOGEI scheme, that would be useful in policy advocacy.

8.1. Key Findings

When training and validating models about autonomous vehicle (AV) environments and behavior, we can draw inspiration from human brain's perception and learning mechanism, shared and integrated with machine learning (ML) (possibly deep learning) approaches. Deep learning models are conceived as "'dark boxes" due to their difficulty in being interpreted. Nevertheless, they have the big advantage to be efficient at inferring from complex input data. Traditional semantic segmentation map representations exhibit a fundamental limit in being unable to represent encoded priorities under uncertainty conditions. On the contrary, depth information needs to be represented in a single semantic map, without loosing the richness and completeness 3D depth information.

The next sections contain the observations discovered during our study [12]. The discussion and recommendations in these sections are based on our verifiable observations and the most relevant studies in the area. This section will present the main findings in the empirical investigation about the relevance and applicability of different human-centered training approaches in the cybersecurity context [9]. The particular focus is given to the perceptions of how beneficial or detrimental four different training intervention methods are in the context of cybersecurity; the findings build on previous recommendations of making training intervention user oriented and engaging, and they present the tested interventions that have not been before discussed in empirical context. Cybersecurity design cannot afford to be generic but must be informed about when and where and why people make mistakes because we are currently far from deploying AI-driven automated security systems.

9. References

[1] Y. Shao, S. Weerdenburg, J. Seifert, H. Paul Urbach et al., "Wavelength-multiplexed Multi-mode EUV Reflection Ptychography based on Automatic-Differentiation," 2023. [PDF]

[2] S. Lee, Y. Cho, and B. C. Min, "Attack-Aware Multi-Sensor Integration Algorithm for Autonomous Vehicle Navigation Systems," 2017. [PDF]

[3] Tatineni, Sumanth. "Exploring the Challenges and Prospects in Data Science and Information Professions." *International Journal of Management (IJM)* 12.2 (2021): 1009-1014.

[4] J. N. Brewer and G. Dimitoglou, "Evaluation of Attack Vectors and Risks in Automobiles and Road Infrastructure," 2020. [PDF]

[5] Vemori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.

[6] L. A. Shepherd, S. De Paoli, and J. Conacher, "Human-Computer Interaction Considerations When Developing Cyber Ranges," 2020. [PDF]

[7] P. Xiong, S. Buffett, S. Iqbal, P. Lamontagne et al., "Towards a Robust and Trustworthy Machine Learning System Development: An Engineering Perspective," 2021. [PDF]

[8] S. M Mostaq Hossain, S. Banik, T. Banik, and A. Md Shibli, "Survey on Security Attacks in Connected and Autonomous Vehicular Systems," 2023. [PDF]

[9] F. Berman, E. Cabrera, A. Jebari, and W. Marrakchi, "The impact universe—a framework for prioritizing the public interest in the Internet of Things," 2022. ncbi.nlm.nih.gov

[10] 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]

[11] 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

[12] A. Shah, "Adversary ML Resilience in Autonomous Driving Through Human Centered Perception Mechanisms," 2023. [PDF]

[13] P. McDaniel and F. Koushanfar, "Secure and Trustworthy Computing 2.0 Vision Statement," 2023. [PDF]

[14] D. Papatsaroucha, Y. Nikoloudakis, I. Kefaloukos, E. Pallis et al., "A Survey on Human and Personality Vulnerability Assessment in Cyber-security: Challenges, Approaches, and Open Issues," 2021. [PDF]

[15] S. Adam Matei and E. Bertino, "Educating for AI Cybersecurity Work and Research: Ethics, Systems Thinking, and Communication Requirements," 2023. [PDF]

[16] F. Sharevski, A. Trowbridge, and J. Westbrook, "Novel Approach for Cybersecurity Workforce Development: A Course in Secure Design," 2018. [PDF]

[17] 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

[18] D. H. Lee, C. M. Kim, H. S. Song, Y. H. Lee et al., "Simulation-Based Cybersecurity Testing and Evaluation Method for Connected Car V2X Application Using Virtual Machine," 2023. ncbi.nlm.nih.gov

[19] M. Hamad and S. Steinhorst, "Security Challenges in Autonomous Systems Design," 2023. [PDF]

[20] T. Holstein, G. Dodig-Crnkovic, and P. Pelliccione, "Ethical and Social Aspects of Self-Driving Cars," 2018. [PDF]

[21] L. Luxmi Dhirani, N. Mukhtiar, B. Shankar Chowdhry, and T. Newe, "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," 2023. ncbi.nlm.nih.gov