frontiers in Psychology

MINI REVIEW
published: 03 May 2019
doi: 10.3389/fpsyg.2019.00995

Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research

Václav Linkov[1], Petr Zámečník[1], Darina Havlíčková[1] and Chih-Wei Pai[2]*

[1] Department of Traffic Psychology, CDV – Transport Research Centre, Brno, Czechia, [2] Graduate Institute of Injury Prevention and Control, College of Public Health, Taipei Medical University, Taipei, Taiwan

The cybersecurity of autonomous vehicles (AVs) is an important emerging area of research in traffic safety. Because human failure is the most common reason for a successful cyberattack, human-factor researchers and psychologists might improve AV cybersecurity by researching how to decrease the probability of a successful attack. We review some areas of research connected to the human factor in cybersecurity and find many potential issues. Psychologists might research the characteristics of people prone to cybersecurity failure, the types of scenarios they fail in and the factors that influence this failure or over-trust of AV. Human behavior during a cyberattack might be researched, as well as how to educate people about cybersecurity. Multitasking has an effect on the ability to defend against a cyberattack and research is needed to set the appropriate policy. Human-resource researchers might investigate the skills required for personnel working in AV cybersecurity and how to detect potential defectors early. The psychological profile of cyber attackers should be investigated to be able to set policies to decrease their motivation. Finally, the decrease of driver's driving skills as a result of using AV and its connection to cybersecurity skills is also worth of research.

Keywords: autonomous vehicle, cybersecurity, human factor, cyberattack, hackers

OPEN ACCESS

Edited by:
Evangelos Himonides, University College London, United Kingdom

Reviewed by:
Stuart Cunningham, Manchester Metropolitan University, United Kingdom
Petra Filkukova, Simula Research Laboratory, Norway

****Correspondence:***
Václav Linkov
vaclav.linkov@hotmail.com;
linkov@email.cz

Specialty section:
This article was submitted to Performance Science, a section of the journal Frontiers in Psychology

Received: *14 December 2018*
Accepted: *15 April 2019*
Published: *03 May 2019*

Citation:
Linkov V, Zámečník P, Havlíčková D and Pai C-W (2019) Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research. Front. Psychol. 10:995. doi: 10.3389/fpsyg.2019.00995

INTRODUCTION

Autonomous vehicles (AV) are vulnerable to many kinds of cyberattacks. The software driving fully AV will have more than 100 million lines of code, so it is impossible to predict the security problems (Parkinson et al., 2017). It is important to study the different ways to attack an AV, the ways to reduce the probability of attacks, and how to minimize the damage. The human is always the weakest point in defending against an attack and dealing with the consequences; therefore, reducing human-induced errors is most effective. Preventing human failure should be taken into account when designing AV (Chong et al., 2018). This is an opportunity for human-factor researchers and psychologists to improve the cybersecurity practices of AV (Proctor and Chen, 2015). In this text, we review how better to protect AV from cyberattacks. First, we discuss the kinds of cyberattacks to which AV is susceptible with focus on those types of attacks where human factor is important. Second, we review the topics studied by psychologists and human-factor researchers to improve cybersecurity and what might be done specifically for AV.

CYBERSECURITY ISSUES IN AUTONOMOUS VEHICLES

There are many ways to initiate an AV cyberattack. An attack can target the software that manages visual information and road infrastructure, or it could be a physical attack on the vehicle's hardware

(Lima et al., 2016). An attack on the remote keyless entry might lock a person inside the car or prevent locking at all (Checkoway et al., 2011). If tire-pressure monitor systems are under the control of an attacker, they might present false readings and hide regular air pressure leakage reduction. An attack on the inclination sensor might cause the car to slow down or start to brake because the sensor signals a steep gradient (Parkinson et al., 2017).

Car communication could be susceptible. The attack could be active, like when the communication is interrupted or replaced by false messages, or it could be passive, like when the attacker gathers information in long-term period for a future malicious purpose (like selling information to some company). Even when the listener cannot decode the data, the time of day the driver uses the car or where the car is located might be still abused (He et al., 2017). There are several types of active attacks on car communication. A spoofing attack is where the attacker uses a false identity or sends false data (e.g., they can pretend that they are a neighboring car or send false information about the neighboring car location). A man-in-the-middle attack is where the attacker gets the original message sent to the car, changes it, and sends the new message to the car (He et al., 2017). A denial of service attack is where the attacker sends a large amount of data to the car so that the communication channel is blocked (Bergin, 2015). Jamming is where a background radio noise blocks the frequency used for communication (Parkinson et al., 2017). A black hole attack is where a message is blocked without informing the car about the missing message (Bergin, 2015). Other types of attacks on AV communication include falsifying the sender's digital signature, forcing the car to restart, and replacing the car communication certificate with a false one (Petit and Shladover, 2014).

The human factor is central for other types of AV attacks. The car information system might be infected by malware, which can cause future damage (Takahashi, 2018), and a human mistake is the most probable source of the infection (e.g., people might download it from the internet). Such an infection might be not direct – the malware (like trojans or viruses) might first infect less-protected systems and advance to the crucial systems (Axelrod, 2017). Cars might also be attacked by putting an infected CD into the CD player, which could automatically download malware (Checkoway et al., 2011). Resulting attack might manifest as a crash of the system which drives the car. Car sharing companies often make people use smartphones to access the car; attacking the smartphone or the communication between the phone and car might be a way the attacker might get into the car (Haas and Möller, 2017). Malware installed through social engineering or car-sharing might lead also to attacks happening during the time when no one is present in the car, so the car might be stolen.

Cybersecurity experts offer plenty of solutions to ensure better AV cybersecurity. Countries should strengthen control of companies producing AV (Lim and Taeihagh, 2018), standardize AV technologies (He et al., 2017), and introduce cybersecurity ranking measures (Burzio et al., 2018). Companies should control products from their suppliers (Parkinson et al., 2017). Different types of communication (Messnarz et al., 2017) and layers of intrusion detection system (Straub et al., 2017) should be mutually independent and each component should have its own firewall (Rizvi et al., 2017). Security system should be often actualized and CAN protected from scanning (Lim et al., 2017). There might be installed chips controlling behavior and temperature of different hardware components to be able to signalize cyberattack (Lima et al., 2016). Also, user interface could be changed to make people more often agree with the cybersecurity-enhancing options (Stavova et al., 2018). If possible, all these mitigation measures should be used simultaneously (Al Mamun et al., 2018).

HUMAN FACTOR IN AUTONOMOUS VEHICLE CYBERSECURITY

Psychologists might help to improve cybersecurity in various ways. People differ in their ability to correctly assess the cybersecurity risk. As found by Yan et al. (2018), 23% of people correctly handle less than half of cybersecurity scenarios; only 4% can handle more than 90% of scenarios. Cybersecurity awareness is a critical issue for AV drivers; therefore, it will be necessary to increase knowledge about cybersecurity for these drivers. Several researchers investigated the characteristics of people with inadequate cybersecurity skills. On the internet, people are prone to behaving in a more risky fashion toward cybersecurity if they are more extraverted, addicted to the internet, impulsive, and less conscientious (Hadlington, 2017). Those who more often use a workplace computer for non-work purposes have less internet security awareness (Hadlington and Parsons, 2017). Men have more experience with cybersecurity than women (Anwar et al., 2017). Anxious people are less successful in detecting a cyberattack (Welk et al., 2015). The characteristics of people with riskier behavior toward AV cybersecurity are yet unknown. The goal for human-factor researchers is to identify the people who are the most vulnerable in AV cybersecurity scenarios, to identify the kinds of scenarios they fail in, and to develop targeted educational materials.

Risky cybersecurity behavior is connected to the over-trust of automated technologies (Noy et al., 2018). When the driver trusts their car too much, it is more prone to attack (Parkinson et al., 2017). An open research question is how to explain these cybersecurity issues to the public and which factors influence the correct recall of this information. People do not understand cybersecurity issues better when the problem is explained metaphorically. A disease-risk metaphor and criminal behavior metaphors do not increase understanding, and a physical assault metaphor worsens it (Brase et al., 2017). The ability to memorize cybersecurity news is moderated by the cyber anxiety of the person: people with higher anxiety related to cyberattacks are bad at retaining cybersecurity-related news (Cheung-Bluden and Ju, 2016).

Engaging in behaviors to enhance cybersecurity is related to the belief that these behaviors are effective and that the cost of the engagement (e.g., time loss) will be minimal (Blythe and Coventry, 2018). People who follow cybersecurity instructions are those who consider ignoring them to be more

risky (Fagan and Khan, 2018). Informing about the risks connected to cyberattacks could be the way to make people to behave more securely.

The level of multitasking in which a driver engages might influence the effectiveness with which they are able react to cybersecurity breaches. People who multitask are prone to risky cybersecurity behavior (Hadlington and Murphy, 2018). Distraction leads to less success in identifying malicious attacks (Kortschot et al., 2018). The ability to react appropriately to a cybersecurity breach is problematic, especially in a transition period, when drivers are not yet used to AV and cognitive overload will be common. Based on research in this field, when AV drivers have to react to unexpected events, they have a wide range of reaction times and the ability to react differs (Gold et al., 2013; Dixit et al., 2016; Dogan et al., 2017). And cybersecurity issues will be more abstract and difficult than real-environment problems. Furthermore, because it is expected that driving skills will decrease with the use of the AVs, number of cybersecurity attacks might rise with time. This raises a question about what amount of distraction and multitasking is acceptable for an AV driver to be able to react to driving issues, not only in general, but especially in terms of cyberattacks. Researchers should provide an answer so that authorities can set appropriate policy.

The frequency of cyberattacks influences human ability to defend against them. Attacks based on social engineering like fishing might be successful only when they are rare. In email communication, when attacks are rare, people are more likely to mistakenly open malicious email. When attacks are more frequent, people trust email less and make fewer mistakes (Sawyer and Hancock, 2018). Researchers should look for a similar relationship for AV usage. They should find what time delay between cyberattack attempts is enough for a driver to lose the ability to react appropriately to cyberattacks, and offer solutions for how to improve drivers' reaction ability. Related issue is the human tendency to lose attention during monotonous task like driving without cognitive involvement of a driver (Saxby et al., 2013) and mitigation of its consequences for readiness to react during cyberattack.

Autonomous vehicles need the authentication of the user (e.g., a password or a passphrase; Juang and Greenstein, 2018). Authentication should be safe; however, it should also be quick and easy to understand so that user can proceed with the proper action quickly. Authentication should also be inclusive and possible for blind people and people with other kinds of impairment. This is a difficult goal (Still et al., 2017) and requires the involvement of human-factor researchers.

Another open issue is how people behave during an AV cyberattack. A cyberattack induces stress in person whose device is attacked (Canetti et al., 2017). When people know that the attacker has adapted to their behavior, they start to behave more randomly (Moisan and Gonzalez, 2017). It is important to research the ways that the car can effectively communicate both the information about the active cyberattack and the appropriate response to an inexperienced driver (Parkinson et al., 2017).

Working in cybersecurity is a very demanding job. The selection of appropriate employees improves cybersecurity culture in an organization and leads to better security decisions (Parsons et al., 2015). Employees should be good team workers and system thinkers. They should also have the necessary technical skills, be able to communicate information to common people, be determined to fulfill their duty, be able to learn continuously (Marble et al., 2015; Dawson and Thomson, 2018), and be well informed about their company's cybersecurity policy (Li et al., 2019). Employees with higher threat awareness and countermeasure awareness perform better in cybersecurity tasks (Torten et al., 2018). Experience from nuclear power plant personnel selection shows that people hired for different positions need different set of skills (Schumacher et al., 2011). Teams that contain people with hostile personality traits perform better in solving cybersecurity scenarios (Cowley et al., 2015), while people with interest in a cybersecurity career tend to have higher self-efficacy and a rational decision-making style (Bashir et al., 2017). Buchler et al. (2018) show that the best performing cybersecurity teams have members who are specialized in specific cybersecurity roles. Specialization brings higher requirements for employee selection. Human-factor researchers should develop procedures that will lead to the effective selection of employees for companies dealing with AV communication infrastructure to ensure maximum safety. Additionally, the percentage of women currently working in cybersecurity in different regions does not exceed 14%, and in Europe it is only 7%, which might be due either to the discrimination women feel in cybersecurity workplaces or bias in selection procedures (Poster, 2018). The selection of employees should address this problem and become less gender biased.

Companies that will be controlling AV cybersecurity must be sure they can trust all of the people in their organizations (Henshel et al., 2015). They should carefully monitor their employees for abuse of their positions (Evans et al., 2016). Hadlington (2018) provides additional suggestions to guard against malicious insiders in an organization – using only trusted connections (e.g., Wi-Fi), using strong passwords, regularly updating software, and limiting personal information shared online. Greitzer and Frincke (2010) suggest keeping tabs on employee stress, disgruntlement, disengagement, disregard for authority, confrontational behavior, dependability, absenteeism, and performance (nevertheless, confrontational behavior might be beneficial for those who should solve and discover cyberattacks – see Cowley et al., 2015). Knowing their personality characteristics and these metrics, the online behavior of employees should be watched and the risk of a cybersecurity breach assessed. When risky behavior is anticipated, the employee should be released from their duties. Greitzer and Frincke (2010) consider such an assessment and its impact on an employee's career to be ethically questionable. Nevertheless, the development of such procedures might become necessary when cyberattacks on the AV infrastructure result in deaths. Such monitoring might be demanding for Human Resources departments and it needs the HR personnel to be continuously educated in these issues (Dreibelbis et al., 2018).

Knowing the motivations and characteristics of attackers might also help to prevent future attacks. King et al. (2018) think that attackers might be characterized by low social status, hyperactivity, socialization toward rule-breaking behavior, and

TABLE 1 | How might human factor researchers improve the cybersecurity of autonomous vehicles (AV).

Security vulnerability	Research goal	Benefit
Characteristics of people who are vulnerable to AV cybersecurity failure is unknown	Identify groups of people who are likely to perform badly in an AV cybersecurity scenario	Vulnerable groups may be targeted by a promotional campaign
Factors that influence human AV cybersecurity performance are not completely known	Identify factors that enhance AV cybersecurity performance	Possible to set policy to increase these factors
Over-trust of AV	Identify groups of people likely to over-trust AV security	Vulnerable groups may be targeted by an educational campaign
AV cybersecurity is problematic and not correctly understood by laypeople	Identify effective ways to explain AV cybersecurity	Educational campaign will increase knowledge
Acceptable multitasking is unknown	Identify acceptable level of multitasking to be able to react to an AV cybersecurity breach	Possible to set policies regarding multitasking for AV
Time when AV cybersecurity defense capability decreases is unknown	Identify period needed to review information about AV cybersecurity	Possible to remind driver after this period
How people behave during specific AV cyberattacks	Understand weak points of people's reactions to cyberattacks	Develop techniques to help laymen during an attack
People working in AV cybersecurity should be able to work in a demanding job	Understand requirements of AV cybersecurity jobs	Develop strategies to correctly select employees for AV cybersecurity
Employees in AV cybersecurity might become attackers or help attackers	Identify detectable behavior changes typical for renegades	Possible to remove risky employees
Characteristics of AV attackers are unknown	Identify who attacks AV and why	Set policies to decrease the motivation of attackers

TABLE 2 | Priority of different human-factor-research related issues in AV cybersecurity in various levels of AV automation as defined by SAE International (2014).

SAE level of automation	(0) No automation	(1) Driver assistance	(2) Partial automation	(3) Conditional automation	(4) High automation	(5) Full automation
Research issue:						
Cybersecurity failure prone people's characteristics	Small	Small	Middle	High	High	Middle
Ways to increase cybersecurity performance	Small	Small	Small	High	High	High
Overtrust to AV	Small	Middle	Middle	High	High	High
Laypeople education	Middle	Middle	Middle	Middle	Middle	Middle
Multitasking acceptability	Small	Middle	Middle	High	High	Small
Cybersecurity defense capability decrease	Small	Small	Middle	High	High	High
Behavior during cyberattacks	Small	Small	High	High	High	High
AV infrastructure companies job requirements	Small	Small	Small	High	High	High
Characteristics of AV cyberattackers	Small	Small	Middle	High	High	High

the dark triad personality traits (psychopathy, narcissism, and machiavellianism). These characteristics might help to develop methods for attacker identification (e.g., analyzing their online social network profiles, methods for successful deterrence of attackers; Lindsay, 2015). Developing specific methods for AV attackers is a goal for future researchers. Such methods would differ for different types of attackers. According to Derrick et al. (2016) attackers could be thieves, organized criminals, political activists, terrorists, foreign government, or vehicle owners themselves. For example, groups of hacktivists might be motivated to participate in cyberattacks to develop a strong identity and the ethos for their group (Thackray et al., 2016). Developing methods to damage the identity of groups that attack AV might help to maintain security.

Cultural differences and specifics should be considered when discussing AV cybersecurity issues. People from cultures with higher uncertainty avoidance, where self-control is preferred over personal desire, might be more prone to ideological indoctrination, such that attack consequences might be exacerbated by the ideological motivation of the attacker. Attackers from cultures with higher long-term orientation might plan more sophisticated attacks (Henshel et al., 2016). These factors should be considered when designing cars for countries with such cultures.

CONCLUDING REMARKS

Cybersecurity research that concerns human factors is still an emerging field (Bordoff et al., 2017). The basic concepts, like cybersecurity culture, are not yet clearly defined (Gcaza and von Solms, 2017). Given that fully autonomous traffic does not yet exist and non-connected autonomous cars exist only in some parts of the world, research on how people behave toward autonomous driving is nearly absent. Psychological researchers might provide a large improvement in the security of AV by investigating these phenomena (Wiederhold, 2014).

There are five types of issues to be researched. First, the characteristics of people vulnerable to AV cybersecurity error and the types of scenarios they fail in. Second, the ways to effectively educate people to improve their AV cybersecurity

skills. Third, how to effectively select and work with employees of companies in charge of AV cybersecurity. Fourth, how to lower the motivation of attackers (see **Table 1**). And, fifth, how the decrease of driving skills as a consequence of autonomous driving will affect the driver's ability to react to cybersecurity issues (nevertheless, it seems that decrease of driving skills is not that large even if person does not drive for long time – see Trösterer et al., 2016).

It is impossible to reach complete cyber safety for AV. Cyberattacks will always happen and some of them will be successful. Therefore, an effective strategy is to not try to eliminate all cyberattacks, but to accept their existence and prepare to react to their consequences (Lin et al., 2016). Some countries, like the United States, China, and Singapore, have already established laws for cybersecurity issues (Taeiagh and Lim, 2018); other countries should follow and prepare for future.

Human-factor researchers should note that changes made to enhance AV cybersecurity might not always increase traffic safety. Macher et al. (2017) gives an example of a situation where a steering wheel is blocked in a dangerous situation. This is safe from a cybersecurity point of view, because the attacker cannot change the steering wheel position. Nevertheless, it is not safe from the position of traffic safety – when a steering wheel is blocked, the driver cannot react appropriately. Researchers should consider these types of situations when designing AV security and think about traffic safety more globally. It should be also noted that cybersecurity threat might be overestimated: Quigley et al. (2015) analyzed texts written by cybersecurity experts and found that many of them use rhetorical techniques to make this threat look larger.

Finally, most of the research suggested here cannot yet be fully conducted, different research issues will be important in different stages of AV automation (see **Table 2**). Research on human behavior when dealing with AV needs to investigate the experience of autonomous driving on common people. Fully AV are not yet widespread, so finding research participants is difficult. Research concerning AV cybersecurity will be more suitable in the future when people will use AV regularly. Nevertheless, researchers should try their best to find what is possible now, because governments and companies should be prepared for the future.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

FUNDING

This manuscript was produced with the financial support of the Ministry of Education, Youth and Sports within National Sustainability Programme I, a project of Transport R&D Centre (LO1610), on a research infrastructure acquired from the Operational Programme Research and Development for Innovations (CZ.1.05/2.1.00/03.0064). C-WP was funded by the joint grants from the Ministry of Science and Technology Taiwan (MOST 105-2221-E-038-013-MY3) and Taipei Medical University (107-3805-006-110).

REFERENCES

Al Mamun, A., Al Mamun, M. A., and Shikfa, A. (2018). "Challenges and Mitigation of Cyber Threat in Automated Vehicle: An Integrated Approach," in *Proceedings of the 2018 International Conference of Electrical and Electronic Technologies for Automotive*, (Milan: IEEE).

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* 69, 437–443. doi: 10.1016/j.chb.2016.12.040

Axelrod, C. W. (2017). "Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks," in *Proceedings of the 2017 IEEE Long Island Systems, Applications and Technology Conference LISAT*, (Farmingdale, NY: IEEE).

Bashir, M., Wee, C., Memon, N., and Guo, B. (2017). Profiling cybersecurity competition participants: self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Comput. Sec.* 65, 153–165. doi: 10.1016/j.cose.2016.10.007

Bergin, D. L. (2015). Cyber-attack and defense simulation framework. *J. Defen. Model. Simul.* 12, 383–392. doi: 10.1177/1548512915593528

Blythe, J. M., and Coventry, L. (2018). Costly but effective: comparing the factors that influence employee anti-malware behaviours. *Comput. Hum. Behav.* 87, 87–97. doi: 10.1016/j.chb.2018.05.023

Bordoff, S., Chen, Q., and Yan, Z. (2017). Cyber attacks, contributing factors, and tackling strategies: the current status of the science of cybersecurity. *Int. J. Cyber Behav. Psychol. Learn.* 7, 68–82. doi: 10.4018/ijcbpl.2017100106

Brase, G. L., Vasserman, E. Y., and Hsu, W. (2017). Do different mental models influence cybersecurity behavior? Evaluations via statistical reasoning performance. *Front. Psychol.* 8:1929. doi: 10.3389/fpsyg.2017.01929

Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., and Lightner, L. (2018). Cyber teaming and role specialization in a cyber security defense competition. *Front. Psychol.* 9:2133. doi: 10.3389/fpsyg.2018.02133

Burzio, G., Cordella, G. F., Colajanni, M., Marchetti, M., and Stabili, D. (2018). "Cybersecurity of Connected Autonomous Vehicles: A ranking based approach," in *Proceedings of the 2018 International Conference of Electrical and Electronic Technologies for Automotive*, (Milan: IEEE).

Canetti, D., Gross, M., Waismel-Manor, I., Levanon, A., and Cohen, H. (2017). How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychol. Behav. Soc. Network.* 20, 72–77. doi: 10.1089/cyber.2016.0338

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., and Shacham, H. (2011). "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX conference on Security*, (Berkeley: USENIX Association).

Cheung-Bluden, V., and Ju, J. (2016). Anxiety as a barrier to information processing in the event of a cyberattack. *Polit. Psychol.* 37, 387–400. doi: 10.1111/pops.12264

Chong, I., Xiong, A., and Proctor, R. W. (2018). Human factors in the privacy and security of the internet of things. *Ergon. Des. Q. Hum. Factors Appl.* (in press). doi: 10.1177/1064804617750321

Cowley, J. A., Nauer, K. S., and Anderson, B. R. (2015). Emergent relationships between team member interpersonal styles and cybersecurity team performance. *Proc. Manufact.* 3, 5110–5117. doi: 10.1016/j.promfg.2015.07.526

Dawson, J., and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Front. Psychol.* 9:744. doi: 10.3389/fpsyg.2018.00744

Derrick, D., Chhawri, S., Eustice, R. M., Ma, D., and Weimerskirch, A. (2016). "Risk assessment for cooperative automated driving," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, Vienna, 47–58.

Dixit, V. V., Chand, S., and Nair, D. J. (2016). Autonomous vehicles: disengagements, accidents and reaction times. *PLoS One* 11:e0168054. doi: 10.1371/journal.pone.0168054

Dogan, E., Rahal, M. C., Deborne, R., Delhomme, P., Kemeny, A., and Perrin, J. (2017). Transition of control in a partially automated vehicle: effects of anticipation and non-driving-related task involvement. *Transport. Res. Part F* 46, 205–215. doi: 10.1016/j.trf.2017.01.012

Dreibelbis, R. C., Martin, J., Coovert, M. D., and Dorsey, D. W. (2018). The looming cybersecurity crisis and what it means for the practice of industrial and organizational psychology. *Industr. Organ. Psychol.* 11, 346–365. doi: 10.1017/iop.2018.3

Evans, M., Maglaras, L. A., He, Y., and Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Secur. Commun. Netw.* 9, 4667–4679. doi: 10.1002/sec.1657

Fagan, M., and Khan, M. M. H. (2018). To follow or not to follow: a study of user motivations around cybersecurity advice. *IEEE Internet Comput.* 22, 25–34. doi: 10.1109/mic.2017.3301619

Gcaza, N., and von Solms, R. (2017). "Cybersecurity Culture: An Ill-Defined Problem," in *Information Security Education for a Global Digital Society. WISE 2017. IFIP Advances in Information and Communication Technology*, Vol. 503, eds M. Bishop, L. Futcher, N. Miloslavskaya, and M. Theocharidou (Cham: Springer).

Gold, C., Dambrock, D., Lorenz, L., and Bengler, K. (2013). „Take over!" how long does it take to get the driver back into the loop? *Proc. Hum. Factors Ergon. Soc. Ann. Meet.* 57, 1938–1942. doi: 10.1007/s10683-015-9468-6

Greitzer, F. L., and Frincke, D. A. (2010). "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation," in *Insider Threats in Cybersecurity*, eds C. H. W. Probst, J. Hunker, D. Gollmann, and M. Bishop (Boston: Springer), 85–113. doi: 10.1007/978-1-4419-7133-3_5

Haas, R. E., and Möller, D. P. F. (2017). "Automotive connectivity, cyber attack scenarios and automotive cyber security," in *Proceedings of the 2017 IEEE International Conference on Electro Information Technology*, (Lincoln, NE: IEEE), 635–639.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* 3:e00346. doi: 10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). "The "Human Factor," in *Cybersecurity," in Psychological and Behavioral Examinations in Cyber Security*, eds J. McAlaney and L. A. Frumkin (Hershey, PA: IGI Global), 46–63.

Hadlington, L., and Murphy, K. (2018). Is media multitasking good for cybersecurity? exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky cybersecurity behaviors. *Cyberpsychol. Behav. Soc. Netw.* 21, 168–172. doi: 10.1089/cyber.2017.0524

Hadlington, L., and Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cybersecur. Behav. Soc. Netw.* 20, 567–571. doi: 10.1089/cyber.2017.0239

He, Q., Meng, X., and Qu, R. (2017). "Survey on Cyber Security of CAV," in *Proceedings of the CPGPS 2017 Forum on Cooperative Positioning and Service*, (Harbin: IEEE).

Henshel, D., Cains, M., Hoffman, B., and Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. *Proc. Manufact.* 3, 1117–1124. doi: 10.1016/j.promfg.2015.07.186

Henshel, D., Sample, C., Cains, M., and Hoffman, B. (2016). "Integrating cultural factors into human factors framework and ontology for cyber attackers," in *Advances in Human Factors in Cybersecurity*, ed. D. Nicholson (Cham: Springer), 123–137. doi: 10.1007/978-3-319-41932-9_11

Juang, K., and Greenstein, J. (2018). Integrating visual mnemonics and input feedback with passphrases to improve the usability and security of digital authentication. *Hum. Fact.* 60, 658–668. doi: 10.1177/0018720818767683

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., and Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Front. Psychol.* 9:39. doi: 10.3389/fpsyg.2018.00039

Kortschot, S. W., Sovilj, D., Jamieson, G. A., Sanner, S., Carrasco, C., and Soh, H. (2018). Measuring and mitigating the costs of attentional switches in active network monitoring for cybersecurity. *Hum. Factors* 60, 962–977. doi: 10.1177/0018720818784107

Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int. J. Inform. Manag.* 45, 13–24. doi: 10.1016/j.ijinfomgt.2018.10.017

Lim, D., Park, K., Choi, D., and Seo, J. (2017). "Analysis on attack scenarios and countermeasures for self-driving car and its infrastructures," in *Advances on Broad-Band Wireless Computing, Communication and Applications, Lecture Notes on Data Engineering and Communication Technologies 2*, eds L. Barolli, et al. (Cham: Springer International Publishing), 429–442. doi: 10.1007/978-3-319-49106-6_42

Lim, H. S. M., and Taeihagh, A. (2018). Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. *Energies* 11:1062. doi: 10.3390/en11051062

Lima, A., Rocha, F., Völp, M., and Esteves-Verissimo, P. (2016). "Towards safe and secure autonomous and cooperative vehicle ecosystems," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, Vienna, 59–70.

Lin, P.-S., Wang, Z., and Guo, R. (2016). "Impact of Connected Vehicles and Autonomous Vehicles on Future Transportation," in *Bridging the East and West: Theories and Practices of Transportation in the Asia Pacific Proceedings of the 11th Asia Pacific Transportation Development Conference and the 29th ICTPA Annual Conference*, (Reston: American Society of Civil Engineers), 46–53.

Lindsay, J. R. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *J. Cybersecur.* 1, 53–67.

Macher, G., Messnarz, R., Armengaud, E., Riel, A., Brenner, E., and Kreiner, C. (2017). "Integrated safety and security development in the automotive domain," in *Proceedings of the WCX^{TM} 17: SAE World Congress Experience*, Detroit.

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., and Sibley, C. (2015). "The human factor in cybersecurity: Robust & intelligent defense," in *Cyber Warfare. Building the Scientific Foundation*, eds S. Jajodia, et al. (Cham: Springer), 173–206. doi: 10.1007/978-3-319-14039-1_9

Messnarz, R., Much, A., Kreiner, C., Biro, M., and Gorner, J. (2017). "Need for the continuous evolution of systems engineering practices for modern vehicle engineering," in *EuroSPI 2017, CCIS 748*, eds J. Stolfa, et al. (Cham: Springer), 439–452. doi: 10.1007/978-3-319-64218-5_36

Moisan, F., and Gonzalez, C. (2017). Security under uncertainty: adaptive attackers are more challenging to human defenders than random attackers. *Front. Psychol.* 8:982. doi: 10.3389/fpsyg.2017.00982

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

Parkinson, S., Ward, P., Wilson, K., and Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Trans. Intel. Transport. Syst.* 18, 2898–2915. doi: 10.1109/tits.2017.2665968

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., and Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *J. Cogn. Eng. Decis. Mak.* 9, 117–129. doi: 10.11124/jbisrir-2015-1072

Petit, J., and Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. *IEEE Trans. Intel. Trans. Syst.* 16, 546–556.

Poster, W. R. (2018). Cybersecurity needs women. *Nature* 555, 577–580. doi: 10.1038/d41586-018-03327-w

Proctor, R. W., and Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Hum. Factors* 57, 721–727. doi: 10.1177/0018720815585906

Quigley, K., Burns, C., and Stallard, K. (2015). 'Cyber Gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Govern. Inform. Q.* 32, 108–117. doi: 10.1016/j.giq.2015.02.001

Rizvi, S., Willet, J., Perino, D., Marasco, S., and Condo, C. (2017). A threat to vehicular cyber security and the urgency for correction. *Proc. Comput. Sci.* 114, 100–105. doi: 10.1016/j.procs.2017.09.021

SAE International (2014). *Automated Vehicles*. Available at: https://web.archive.org/web/20170903105244/https://www.sae.org/misc/pdfs/automated_driving.pdf (accessed October 17, 2017).

Sawyer, B. D., and Hancock, P. A. (2018). Hacking the human: the prevalence paradox in cybersecurity. *Hum. Factors* 60, 597–609. doi: 10.1177/0018720818780472

Saxby, D. J., Matthews, G., Warm, J. S., Hitchcock, E. M., and Neubauer, C. (2013). Active and passive fatigue in simulated driving: discriminating styles of workload regulation and their safety impacts. *J. Exp. Psychol. Appl.* 19, 287–300. doi: 10.1037/a0034386

Schumacher, S., Kleinmann, M., and Melchers, K. G. (2011). Job requirements for control room jobs in nuclear power plants. *Saf. Sci.* 49, 394–405. doi: 10.1016/j.ssci.2010.10.002

Stavova, V., Dedkova, L., Matyas, V., Just, M., Smahel, D., and Ukrop, M. (2018). Experimental large-scale review ofattractors for detection of potentially unwanted applications. *Comput. Secur.* 76, 92–100. doi: 10.1016/j.cose.2018.02.017

Still, J. D., Cain, A., and Schuster, D. (2017). Human-centered authentication guidelines. *Inform. Comput. Secur.* 25, 437–453.

Straub, J., McMillan, J., Yaniero, B., Schumacher, M., Almosalami, A., Boatey, K., et al. (2017). "CyberSecurity considerations for an interconnected self-driving car system of systems," in *Proceedings of the 2017 12th System of Systems Engineering Conference (SoSE)*, (Waikoloa, HI: IEEE).

Taeiagh, A., and Lim, H. S. M. (2018). Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Trans. Rev.* 39, 103–128. doi: 10.1080/01441647.2018.1494640

Takahashi, J. (2018). An overview of cyber security for connected vehicles. *IEICE Trans. Inform. Syst.* E101, 2561–2575. doi: 10.1587/transinf.2017ici0001

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., and Richardson, C. (2016). "Social psychology: An under-used tool in cybersecurity," in *Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI '16*, Poole.

Torten, R., Reaiche, C., and Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Comput. Secur.* 79, 68–79. doi: 10.1016/j.cose.2018.08.007

Trösterer, S., Gärtner, M., Mirnig, A., Meschsterjakov, A., McCall, R., Louveton, N., et al. (2016). "You Never Forget How to Drive: Driver Skilling and Deskilling in the Advent of Autonomous Vehicles," in *Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, Ann Arbor, MI, 209–216.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., and Mayhorn, C. B. (2015). Will the "phisher-men" reel you in? Assessing individual differences in a phishing detection task. *Int. J. Cyber Behav. Psychol. Learn.* 5, 1–16. doi: 10.4018/IJCBPL.2015100101

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cybersecur. Behav. Soc. Netw.* 17, 131–132. doi: 10.1089/cyber.2014.1502

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., et al. (2018). Finding the weakes links in the weakest link: how well do undergraduate students make cybersecurity judgment? *Comput. Hum. Behav.* 84, 375–382. doi: 10.1016/j.chb.2018.02.019

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.