IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 28, Issue 2, Series 7 (February, 2023) 35-42
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Trends in Automobile Hacking: A Critical Analysis of its Ramifications and the Role of Law

Samuel Philip Minas R[1], Nanthieswar Sathian[2]
[1](Department of Criminology, Karunya Institute of Technology and Sciences, India)
[2](Department of Criminology, Karunya Institute of Technology and Sciences, India)

Abstract: The advent of technological development in the automobile industry over the course of two and a half decades has reached a pinnacle of advancement in not just transportation but also the tools and instruments that make transportation easier. This article delves into the vulnerabilities that are found in such technological advancement. The article consists of a detailed analysis of the possible threats in automobile hacking and the way in which it can be used by fringe and extreme elements in the society to engage in criminal activities. The Bluetooth, GPS software, onboard vehicle diagnostics, braking and throttling systems in modern vehicles are certain vulnerabilities which have been exploited by cybercriminals. From a Criminological perspective, the absence of guardianship (like a competent legislative act) as propagated by the Routine Activity Theory makes automobiles a more suitable tool for commission of cybercrimes by exploiting the technology available in them. This paper has critically analyzed and compared various legislation pertaining to motor vehicles and if they are competent enough to tackle cyber-crimes and crimes committed through, and in a motor vehicle. This paper also aims at understanding the complexities of identifying, apprehending and punishing the individuals who commit such crimes. The anonymity provided by cyberspace has made it difficult to track down perpetrators who employ various means to mask their identity while committing such crimes. The challenges faced by the Criminal Justice System in meting out punishments for such cases is the focus of research in contemporary times. The data for this paper was gathered through content analysis techniques and comparative studies and secondary data that was available on a plethora of journals, websites and books.

Background:Technological development in the automobile industry has paved way for greater transportation services but at the same time has also fallen prey to extensive crimes, and off-late, cyber crimes. This paper looks at the different ways in which the modern vehicles are prone to hacking and what are the effective means of tackling such crimes and the necessary legislative changes that have to brought in to deal with it.

Materials and Methods: This research takes an explorative approach to the topic of automobile hacking and the role of law in dealing with cybercrime pertaining to automobiles. It is exploratory in nature as it seeks to understand the problems or vulnerabilities in technologically advanced vehicles and the extensive role played by legislative acts in dealing with crimes committed using such vehicles. The data collection method used is secondary in nature. This implies the use of available research and archival data from various online and offline sources such as journals, articles and books.

Conclusion: The existing mechanisms to counter such crimes are effective only to a certain extent and are hard to be universally applied. Even though countries have the choice of introducing their own legislations, there is not enough research done before implementing such rules and regulations. The cyberspace is a vast abyss and finding out who perpetrated a crime is really difficult. The day-to-day advancement of spyware and location hiding tools and software's are only aiding and encouraging such criminals. Therefore, to prevent the rise of automobile hacking and to reduce the damages that it can cause, we must be prepared to face the challenges by adopting and implementing effective action plans that are carefully meted out and are based on solid research and thorough continuous assessments.

Key Word: Automobile hacking, cybercrime, motor vehicle legislations, criminal justice system

---

Date of Submission: 11-02-2023 Date of Acceptance: 22-02-2023

I. Introduction

The advent of technological development in the automobile industry over the course of two and a half decades has reached a pinnacle of advancement in not just transportation but also the tools and instruments that make transportation easier. This development though serves as one of the greatest achievements of mankind, it brought about serious ramifications of its own. This technology proved to be a huge vulnerability which exposed

automobiles to exploitation through unauthorized remote access control. Such unauthorized access can be used for various purposes that can harm an individual or even a group of people and at the worst threaten the stability of a state or an organization. Cybercrimes have been a topic of debate and contemplation for almost a decade but it was just pertaining to computer networks, the computer and the internet. However, the impact of computers and the internet in the automobile industry has opened a new avenue for debate which focuses on the computerization of automobiles and inclusion of technologically advanced instruments and accessories that control the vehicle. Since cybercrimes have made identification of offenders a very strenuous task, the law plays an important role in defining such crimes, criminals and the punishments. The existing laws are not sufficient to regulate contemporary crimes in cyberspace. The lack of specificity in defining crimes pertaining to cyberspace is a big loophole. Therefore, amendment of existing laws and introducing new legislative acts corresponding to cybercrimes and motor vehicles are an urgent need of the hour.

As indicated by Interpol, vehicle crimes include everything from theft to unlawful distribution of car spare parts and car accessories. Automobile hackers exploit vulnerabilities in the vehicle's equipment, software or PC networks that are associated with communication and GPS tracking. Besides, with a stronger network connectivity comes a greater risk of cyber-attacks. This is on the grounds that the latest models of vehicles have many new amenities, better infotainment frameworks and beneficial safety measures and precautions that make driving simpler and more pleasant. Due to all these changes vehicles have now come to be seen as a supercomputer. Therefore, they are at a more serious level of threat and harm by viruses, bugs, phishing and hacking like any other computer system. These viruses and other malwares can cause serious damage to the vehicle's software which in turn can hamper the performance of the vehicle.

The most nerve-racking challenges faced by the automobile industry is to develop and improvise the safety and security systems in vehicles. Automobile hacking is one of the biggest threats faced by these industries. The hacker has full control of the car and can access the features hands free from any place they are in. These industries aim to design security systems for the cars and upgrade them to their upcoming new models. These systems are of high standards and technologically advanced, yet they fail to achieve the goal and the hacker gains access to the vehicle1. The very important part of accessing a vehicle is the authentication factor. When a stranger tries to open the car, a pin or key is needed to check the authentication of the person. There are times when the security system turns futile and causes jeopardy. Notifying the owner when their car is being accessed will help prevent any mishap. Designing such secured systems will help prevent further crimes. Studies have shown that 'hacktivist' gain information through On-BoardDiagnostic (OBD) interface which helps in systematically deriving data from the in- vehicle system. (2)

Technology plays an important role in cyber hacking. As much as its needed, it has its odds too. With the advancement of 4G LTE and 5G communication technology hackers find their ways to collect data from vehicles. Intelligent automobiles have advanced automated systems that open up opportunities for cyber-crime including in-vehicle attacks and vehicle-to-everything communications attacks. A study which analyzed the major attacks on intelligent connected vehicles classified them into four categories namely cryptography, network security, software vulnerability detection, and malware detection. Working on these categories will help in securing the systems.(2)

Globally rapid acquisition of ADAS (An advanced driver-assistance system), internet-connected and the lay-out of semiautonomous to self-driving cars on roadways, cyber security for smart cars with advanced electronics is perturbed with time. An article shows a step-by-step methodology of car hacking research and to show their lab mates, colleagues and students how their cars get hacked in lab environments. Academia plays a role by introducing courses that allow students to learn about hacking and cybersecurity systems, which will enable them to become more aware of how these technologies function. The work exhibits how an automobile is tested for its vulnerabilities that imply replay attacks, reverse-engineer CAN bus messages, by combining an open-source tool and a commodity CAN-to-USB cable. CAN (controller area network) is a system used in modern automobiles. (2)

The cultivation of technology in automobiles over the years has created a new type of "on the road" entertainment and safer environment while driving. To obliterate the dangers caused while driving, varied technologies like anti-lock brake systems, steering assist, and in some cases autonomous driving have been designed by manufacturers. A strong security system will enable safety to the vehicle and thus the need to develop safe technologies.(3)

Modern vehicles are basically entities of information systems. As the vehicle gets more computerized, directly proportional is the attack of them. As research in security services and studies show the weakness and vulnerability of these systems, it is evident that motorized builders haven't emphasized on developing a secured vehicular information system. In fact, the field of automobile industry is at the onset of growing. An article showing the vulnerability of the security system including the access to the head unit and control the physical aspects of the driving subsystem, along with the steering and braking was demonstrated by Miller and Valasek in 2015 where they managed to remotely compromise a 2014 Jeep Cherokee (3).

To understand the pressures linked with modern vehicles the federal fleet managers along with the information technology team work together. As vehicles become safer wholly, the dangers shift from distracted drivers to privacy interference and compromised operation. Most of the time federal fleet managers cannot execute mitigation recommendations on their own, instead they need to discuss and work with the team members and network providers guaranteeing that security measures are embodied into the technology. In order to protect driver safety and data privacy for connected and automated vehicles (CAVs), telematics, and electric vehicle supply equipment (EVSE), a report pins down the security concerns, mitigation techniques, and procurement language that can be studied (4).

Setting passwords for/ on our phones, cars, doors at the office or our homes is the need for today. With robbery, crimes, and foul play happening every now and then, security systems have to be tight to secure our valuables with utmost care. Traditional lock system has been outdated and the digital lock system has taken its stand worldwide. A project "Password Based Door Locking System" using an Arduino showed effective use in security fields. These doors locking security systems are used in our Houses, Institutions, Banks and any Public Places. Only when the correct password is entered the door opens an incorrect password doesn't pave entry to the person as it appears invalid on the display screen (2).

With the rise in thefts and the need for security systems technology is becoming innovative with the use of its tools and software in automobile industries. Increasing the modules inside the vehicle and systematically controlled by monitors that are reported to remote systems. The use of monitors and interconnected systems which will be the future of the automobile industry will make researchers develop better prototypes to mitigate, detect and protect the systems(3).

The future of vehicle technology is one of increasing use of computers and interconnected systems, which demands researchers develop models to detect, mitigate, and protect these systems from agreements (3).

Considering the hazards for cybersecurity, three main concerns must be looked into. Firstly, security of the device that is being hacked- be it mobile, laptop, sensitive data or a vehicle. Threats targeting data and computer systems surfing from malwares and guessing passwords that gain access to the systems. The second factor is data security as it plays an important role in protecting the system from internal and external threats. And lastly cost and energy required to safeguard the system from such threats (4).

Our automobile industries should help us keep our valuables 'Safe and secure'. The need to analyze and develop secured systems for vehicles in a systematized manner is the most important area of research in today's world. There are different digital methods to secure the systems which can be studied, planned, designed and executed by the research team. Being alerted when a hacker attacks your system and reporting the issue immediately to cybersecurity, will and should be the first choice. Legally following laws and protocols will make it easy to prevent and retrieve stolen data or vehicles.

II. Material And Methods

Aims and Objectives-To identify the vulnerabilities in technologically advanced vehicles.To understand the complexities of identifying, apprehending and punishing individuals who exploit the vulnerabilities to commit crimes.To acknowledge the need and role of Law to tackle such crimes.

Study Design: This research takes an explorative approach to the topic of automobile hacking and the role of law in dealing with cybercrime pertaining to automobiles. It is exploratory in nature as it seeks to understand the problems or vulnerabilities in technologically advanced vehicles and the extensive role played by legislative acts in dealing with crimes committed using such vehicles.

Study Duration: April 2022 to May 2022.

III. Analysis and Interpretation

Plausible vulnerabilities that can be exploited

When it comes to technological development in the automobile industry, the first big name that pops up is Tesla. But, no matter how successful or advanced the vehicle is, it does not mean that it is perfect. Recent studies by LennertWouters show that Tesla's Model X is easily hackable via bluetooth. The keyless entry system that Tesla has adopted has posed a big cybersecurity risk. This form of vehicle entry is done via Bluetooth. The vehicle uses over the air system to connect to the owner's phone via Bluetooth which therefore exposes the frequency signal to hacking. Hackers can use various devices to intercept the Bluetooth transmission and reprogram the code and gain access to the vehicle[3].

The On-Board Diagnostics, in short OBD, interface in a car empowers an effective method for accessing information of the vehicle electronic system and leaves way for unapproved access by a hacker. On-board-diagnostics monitors emissions, mileage, speed, and other helpful information about the vehicles. It is programmed to check engine light, which blinks when the system identifies an issue. On one hand, OBD empowers digital access to public information, for example to emission control and blunder codes and on the

other hand, OBD empowers access additionally to confidential details embedded by the manufacturer and the explicit electronic control unit settings, for example to robbery protection or engine control.

Utilizing a Wi-Fi hot-spot malignant individuals can get subtleties of the vehicle like its make and model. Besides, it likewise becomes workable for them to get their hands into the IP address of the vehicle's PC framework. Alongside this, they can likewise identify the vehicle's location through its GPS. Despite the fact that this may be a remote chance, programmers could try and control the vehicle's GPS location.

Researchers from the University of Michigan put forth their discoveries of an upsetting arrangement of tests on modern vehicles. By conveying computerized messages inside the internal network of a truck, the researchers had the option to do all actions from changing the readout of the truck's instrument board, trigger acceleration, or to try and impair one type of the semi-trailer brakes. Furthermore, the scientists found that fostering these attacks were really simpler than with cars, because of a typical form of communication technology standard in the internal network of most modern vehicles, from concrete blenders to heavy transport vehicles[4].

The above mentioned are just a few ways in which one can hack and exploit an automobile. Opportunities to hack an automobile are endless and as time progresses the various ways in which one can hack into them are also increasing.

Lack of Competent Legislation

Counter measures for such crimes need to be introduced through either new legislation or by updating and amending the existing laws. For example, in India, there is a special act for motor vehicles called, The Motor Vehicles Act, 1988. This act covers all aspects of regulating and monitoring the use of motor vehicles and the documentations required. It also lays down rules and laws regarding traffic regulations and penalties and fines associated with violation of these rules[5]. On the other hand, the Information Technology Act, 2000 was introduced in order to provide a legal framework for e-commerce and electronic data transfers and transactions. The act covers all activities that take place in the digital or electronic form, basically the cyberspace[6].

However, when it comes to the topic of research, it shows that there is no proper legislation covering the aspect of automobile hacking and the associated threats and risks. It is true that the concept of automobile hacking is new and studies are still being conducted in this particular area to gain a better understanding of the danger it poses, but, the recent developments in the automobile industry which is digitally and electronically revolutionizing the components of an automobile is also opening pathways for cyber criminals to misuse this technology. Therefore, in order to prepare for the worst there has to be competent legislation to monitor and regulate such activities. This legislation must contain aspects of both, The Motor Vehicle Act and the Information Technology Act, and specifically cover all aspects of the use of modern vehicles including punishments and penalties for misuse of such vehicles for criminal activities.

The importance for implementation of such acts has been acknowledged by various international organizations, most importantly the United Nations and the European Union. Two new UN Regulations on Cybersecurity and Software Updates will assist with handling these dangers by laying out clear execution and review prerequisites for vehicle manufacturing companies. These are the very first universally fit and restricting standards pertaining to automobile cybersecurity.

The regulations recommend the application of the measures across four major disciplines. They are,

1. Overseeing vehicle cyber threats and risks.

2. Modifying or designing the vehicles in such a way that such risks and threats are reduced. Recognizing and reverting to security issues in the vehicles.

3. Giving completely safe software programming updates and guaranteeing vehicle safety isn't compromised.

4. Presenting a lawful reason for purported over-the-air updates to on-board vehicle programming.

These regulations have been proposed for all kinds of cars, trucks, vans and other road transport vehicles. However, other forms of transport via air and sea are still in debate. Various countries including Japan, South Korea and the European Union have shown interest in adapting and implementing these regulations. South Korea is following a step-by-step approach in slowly integrating these guidelines as laws as time progresses. These provisions and guidelines will include regulations on Cybersecurity and how it will be implemented. In the European Union, all new regulations adopted from the UN will be made mandatory for all vehicles from July of 2022. This move by the UN has not only helped in initiating the first step towards automobile cybersecurity but has also opened a vast market for investment in this area of research and development[7].

Complexity in Punishments

The most challenging part about dealing with cybercrimes are the complexities in identifying, apprehending and punishing the individuals who commit such crimes. There can be a compulsion to see cybercrime as a practically undetectable peculiarity. Attacks happen through the internet and are organized by

inconspicuous and obscure individuals. In such cases, only information regarding victims is available and not of the perpetrators. This prompts a perplexity of cybercrime and an emphasis on the technical parts instead of the offenders, which makes the peculiarity much more unfamiliar to the common man. The truth, obviously, is fairly unique.

Yet, the origin of cybercrime as an industry is more about the manner in which it operates, as opposed to the money it generates for the cyber criminals and costs its victims. While one can become caught in a definitional entanglement, in basic terms an industry comprises organizations that work in comparative ways and produce similar kinds of labor and product. While its labor and products are generally unlawful, the cybercrime business works as per similar expansive standards of modern association seen across various different settings. In the first place, there is a reasonable division of work, with various cybercriminal who rose to fame from hacking, to coding, to distributing, they were successful in transforming virtual incentives into financial gains.

These strengths have underlying specialties. The danger is as of now not simply solitary programmers working for amusement, however, incorporate significantly more expert offenders or criminals who are driven by monetary inspirations. The rising specialization of cybercriminals is reflected by the development of online business sectors. In such a manner, virtual commercial centers, which to some degree look like criminal business centers, have become especially significant. In every one of these marketplaces, a huge number of cybercriminals can meet and exchange illegal goods and services online. Normal items that are exchanged incorporate compromised debit and credit card information, online banking logins and malware. At last, cybercriminals progressively work together in groups, which to some degree starts to look like a business organization. Most of these groups include a small number of individuals working with specifically assigned roles. They could deliver malware collectively or convey intricate schemes online. Their uttermost mark of complexity is that a portion of these organizations are practically indistinct from actual organizations, with actual office space and corporate structures.

When it comes to automobile hacking, it is very difficult to understand who will be liable for the crime. The owner of the vehicle or the one who hacked into the vehicle. The owner of the vehicle is liable for all activities their vehicle is used for but at the same time, proving whether they know that their vehicle was hacked will pose a challenge to the investigators. The burden of proof therefore lies on the owner to prove that they are not involved in the crime. The offender however, using the mask provided by cyberspace can easily cover up their tracks and act like nothing ever happened. This further puts the owner of the vehicle at a risk of being falsely accused. Therefore, this brings in the question if the vehicle manufacturing companies should also be liable for lapses in their vehicle's software and security measures. This is a great challenge for the criminal justice institutions when it comes to investigating such crimes and apprehending the offender and initiating a trial and to convict the same. This calls for technologically improving investigative techniques to further get closer to catching the offender without draining much of the existing resources. Wasting time focusing on one case will only delay the cases that are piling up one after the other. This therefore drags and delays investigation, trial, judgments and convictions for all such cases, therefore making the criminal justice system look incompetent and helpless.

Applying the Routine Activity Theory of Crime

Not sufficient data is generated about criminological literature regarding examining vehicle cybersecurity and methods of prevention that can be used. According to (Cohen and Felson 1979) RAT (routine activity theory) in particular furnishes a summary of ways to analyze and study mitigation or prevention of vehicle cybersecurity risks[8].

Lawrence Cohen and Marcus Felson put forth a theory of crime called Routine Activity Theory. This theory is one of the opportunity-based crime theories which talks about how a crime is committed based on assessing situational factors. It talks about how crime is more of an event that occurs in different stages by careful consideration of environmental and social factors. Crime happens while the following three elements come together, a motivated offender, a suitable target and the shortfall of a capable guardian. This hypothesis incorporates the routinely executed and observed activities of both offender and victim. For example, an offender has locked a specific target and observes the daily routine of the target for the purpose of finding out the places the target travels. This target owns a modern car with the latest technologies. The offender tries to understand the vulnerabilities of the vehicle by closely monitoring the activities of the target and how the vehicle is left unguarded for a specific time period during the day or night. At the right time, with the use of proper aids, he is able to successfully hack the vehicle without the target's knowledge and that too remotely. Therefore, the lack of a proper guardian for the vehicle enabled the offender to utilize the opportunity and commit the crime.

On the other hand, from a judicial perspective, the lack of a capable legislative guardian can further encourage cyber criminals to engage in such criminal activities. Scholars have studied that existing civil liability

law will mostly be malleable, adapting to most of the legal claims caused by technologically advanced vehicles. Every person involved in the automobile industries that design these vehicles starting from the manufacturers, owners, insurers, policymakers, and others should take into consideration the risks, their liability implications, and both regulatory and statutory policy responses and must be aware of the lawsuits[9].

IV. Result and Critical Analysis

Identifying the offender

As we have seen earlier, identifying the offender is one the greatest challenges of cybercrimes. The dark web is the greatest shield for any cybercriminal. It acts as a huge wall of defense for criminals engaging in such criminal activities. This however is not the case all the time. Advanced technology for aiding as investigation tools have enabled investigating authorities to identify criminals a bit faster than before. However, with the ever-evolving technology, the trend is always that the bad guy gets a hold of the good technology before the law enforcement authorities. The biggest question that arises is who should be punished and for what? Even though the crime has occurred, it will be difficult to identify who committed the crime. The vehicles being registered in the owner's name, the liability of the crime also falls on the owner. The owner might be completely unaware of such activity due to lack of knowledge or proper security measures, but they still have to pay the price for not safeguarding their vehicle through proper means and therefore being the victim of the crime as well. The enigma this situation creates is a big challenge to distinguish between the offender and the victim and who and how much they should be punished.

In order to combat this, the legislations and policies must clearly and extensively define the following-

Who is the offender?

- The liability of the owner of the vehicle.
- Liability of the vehicle manufacturing companies.
- The degree of punishments that will be awarded for the crime, depending on its intensity.
- The impact of the crime committed.
- The perceived threat to cyberspace and the community.

Problem with legislation

Crime evolves faster than the criminal justice system. The criminal justice system is more reactive to crimes than being proactive. This therefore pushes the criminal justice system a few steps back when it comes to dealing with cyber criminals. Even though automobile hacking and related crimes are minimal in India, we need to prepare for such complications. Every time a bill, law or an act is passed, it requires a team of expert policy makers who scrutinize and explore all information pertaining to the problem. Adequate research is mandatory and constant updating and amendment of laws must also be done. If there is a lack of such expertise, it becomes difficult to introduce effective and well-defined legislation. As discussed in the Routine Activity Theory, the lack of a capable guardian only fosters the occurrence of a crime. Therefore, if there are no laws regarding automobile hacking and other crimes relating to technologically advanced vehicles, it will cause great difficulty in monitoring, regulating and preventing such crimes. A permanent committee which includes policy makers of the state, representatives of all automobile manufacturing company which are technologically revolutionizing the industry and experts in the field of cyber security will be beneficial.

Scope for other crimes in the future

The existing lacunas in vehicle security can be used by anti-social elements and groups in the society to use hacked automobiles as tools for committing crimes including but not limited to terrorism, car high-jacking and theft, espionage and infringement of right to privacy.

Talking about terrorism, the modern vehicles can be easily manipulated remotely and used by terrorist organizations to further their plans and actions by using these vehicles armed with IED's as car bombs. The research and introduction of autonomous vehicles with driverless and self-driving technology will only make it easier for such organizations to use these vehicles for terrorist activities. It will allow these organizations to remotely control such vehicles and use them to disturb public tranquility and peace. Remote access can enable criminals to override and control a vehicle's onboard diagnostics without the owner's knowledge. Once they gain access to the vehicle's system, they can manipulate the vehicle and disable its alarm and security features allowing them to steal the vehicle manually and also gain access to the personal information of the vehicle's owner.

The development of voice recognition command technology in vehicles has begun to be used as a tool for collecting information. The Bluetooth and GPS tracking systems which have voice command functions enable the owner to control and give commands for certain actions while driving the vehicle. The mics in these systems can be easily hacked and used to listen to the conversations in the vehicle. This will therefore invade the privacy of individuals. This can be used for espionage purposes, especially to collect information from

prominent and high-profile individuals who can be a source of valuable information in the private or public sector.

The United Nations put forth its regulations on cyber security and software updates for technologically advanced vehicles in the year 2020. As we saw earlier under lack of competent legislations, despite calling for changes in the four major dimensions of monitoring, modifying, securing the software and introducing globalized on-the-air connection systems, the major obstacle in this proposal is that this plan is more feasible for the developed nations, and we must not forget that the developing nations also form a major part of the United Nations. The regulations are more general than specific and just put forth a loose framework for the countries to build on. This will only make things worse by putting more pressure on the legislative bodies of the developing countries. Moreover, giving the countries a free hand to put forth laws according to their needs can further cause problems to the manufacturers as each country will have its own needs and changing vehicle design and software to suit each country will be a hectic work. The developed countries have time and means to combat such problems but the developing nations have to overcome a plethora of impediments to even adopt and implement such regulations.

Modernized vehicles are still finding solid ground to establish themselves in developing countries. Another problem that can be found here is that car manufacturing companies look for developing countries to establish their manufacturing facilities to reduce labor costs and mitigate extra expenses. This further creates loopholes in building the car and fitting of cheap components will only make the vehicle more vulnerable to all forms of threats.

V. Discussion and Conclusion

Through the research, it was found that the development of the automobile industry has helped humanity to reach a stage of technological development that could not have been possible to even think of 25 years ago. The development has significantly impacted humanity in a positive way and has pushed the whole system of transportation to another level. However, every boon has its own bane. This bane has come in the form of technological development in automobiles and the persistent growth of cybercrimes. The existing mechanisms to counter such crimes are effective only to a certain extent and are hard to be universally applied. Even though countries have the choice of introducing their own legislations, there is not enough research done before implementing such rules and regulations. The cyberspace is a vast abyss and finding out who perpetrated a crime is really difficult. The day-to-day advancement of spyware and location hiding tools and software's are only aiding and encouraging such criminals. Another problem is that each vehicle manufacturer has their own software's and technologies that differ widely from the pre-existing ones in the market. This will only make setting up effective tackling strategies more strenuous. Therefore, to prevent the rise of automobile hacking and to reduce the damages that it can cause, we must be prepared to face the challenges by adopting and implementing effective action plans that are carefully meted out and are based on solid research and thorough continuous assessments.

References

[1]. Aastha Yadav and others, 'Security, Vulnerability and Protection of Vehicular On-Board Diagnostics' (2016) 10 International Journal of Security and Its Applications 405 http://article.nadiapub.com/IJSIA/vol10_no4/36.pdf accessed 26 May 2022.

[2]. Admin, "Password Based Digital Door Lock Security System Using Arduino and Keypad " Electroduino" (*ElectroDuino*October 20, 2021) https://www.electroduino.com/password-based-door-lock-security-system-using-arduino/ accessed 28 May 2022

[3]. "Car Hacking: Accessing and Exploiting The Can Bus Protocol" https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1045&context=jcerp

[4]. Currie R, "Developments in Car Hacking" (*Semantic Scholar*January 1, 1970) https://www.semanticscholar.org/paper/Developments-in-Car-Hacking-Currie/2774f43fb591c853b91418fcf61e838181e5e510> accessed 26 May 2022

[5]. Gerla M and others, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds" [2014] 2014 IEEE World Forum on Internet of Things (WF-IoT)

[6]. Greenberg A, "This Bluetooth Attack Can Steal a Tesla Model X in Minutes" (WiredNovember 23, 2020) https://www.wired.com/story/tesla-model-x-hack bluetooth/ accessed 28 May 2022

[7]. Greenberg A, "Hackers Hijack a Big Rig Truck's Accelerator and Brakes" (WiredAugust 2, 2016) https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/ accessed 28 May 2022

[8]. Hodge C and others, "Vehicle Cybersecurity Threats and Mitigation Approaches"

[9]. Jay Kennedy, Thomas Holt and Betty Cheng, 'Automotive Cybersecurity: Assessing a New Platform for Cybercrime and Malicious Hacking' (2019) 42 Journal of Crime and Justice 632 <https://www.tandfonline.com/doi/full/10.1080/0735648X.2019.1692425> accessed 26 May 2022.
[10]. Leukfeldt ER and Yar M, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis" (2016) 37 Deviant Behavior 263
[11]. "Manipulating Car Diagnostics and Mechanics through Cyber Attacks" <https://www.irjet.net/archives/V8/i8/IRJET-V8I8477.pdf>
[12]. Mahdi Dibaei and others, 'Attacks and Defences on Intelligent Connected Vehicles: A Survey' (2020) 6 Digital Communications and Networks 399 <https://linkinghub.elsevier.com/retrieve/pii/S235286481930197X> accessed 26 May 2022.
[13]. "Remote Exploitation of an Unaltered Passenger Vehicle" <https://www.illmatics.com/Remote%20Car%20Hacking.pdf> accessed 28 May 2022
[14]. Syed Rizvi and others, 'A Threat to Vehicular Cyber Security and the Urgency for Correction' (2017) 114 Procedia Computer Science 100 https://linkinghub.elsevier.com/retrieve/pii/S187705091731815X accessed 26 May 2022.
[15]. The Information Technology Act, 2000 (Amended in 2008)
[16]. The Motor Vehicles Act, 1988 (Amended in 2022)
[17]. "UN Regulations on Cybersecurity and Software Updates to Pave the Way for Mass Roll out of Connected Vehicles" (*UNECE* June 24, 2020) <https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll>
[18]. Winkelman Z and others, "Hacked Autonomous Vehicles: Who May Be Liable for Damages? an Initial Investigation into How Civil Liability Systems Can Prepare"

Samuel Philip Minas R, et. al. "Trends in Automobile Hacking: A Critical Analysis of its Ramifications and the Role of Law." *IOSR Journal of Humanities and Social Science (IOSR-JHSS)*, 28(2), 2023, pp. 35-42.