AARMS Vol. 23, No. 2 (2024) 63–75.

10.32565/aarms.2024.2.5

Cybersecurity Challenges in the Era of Chinese Electric Passenger Vehicles

A Qualitative Study Investigating Data Security Measures in the European Union

Henrietta HEGYI[1]

The present research focuses on investigating the security of data transmitted by electric passenger vehicles originating from the People's Republic of China, particularly when sent for remote processing. Initially, the study examines the factors contributing to the widespread presence of Chinese vehicles in the European market. Additionally, it explores the measures undertaken by the European Union to safeguard the information and data security of its member states. Following this investigation, an in-depth qualitative research method involving semi-structured interviews was conducted. Ten experts in information security were interviewed, and their insights were analysed concerning the identified challenges. The primary objective of this publication is to draw attention to the conceptual deficiencies that impede the protection of data and information, highlighting how a large volume of data collected from a third country, in this case, electric passenger vehicles, may pose national security risks.

Keywords: *qualitative research, cybersecurity, passenger car, information security, data security*

Introduction

In contemporary times, the passenger vehicles utilised bear little resemblance to those of ten to twenty years ago. The industry has undergone significant evolution, with various convenience and safety functions offered by information technology solutions swiftly assuming a leading role in the vehicles' sales considerations. Present-day automobiles, equipped with specialised sensors, gather copious amounts of data, not only about their own technical parameters but also about the passengers and their surroundings. The European Union (and the world at large) endeavours to manage this process through various regulations and standards; however, the rapid pace of technological advancement and ensuing changes present challenges. This poses difficulties for local automotive

[1] PhD student, Óbuda University, e-mail: hegyi.henrietta@uni-obuda.hu

manufacturers and stakeholders in ensuring compliance with regulations. Nevertheless, due to the absence of a global central authority, there is even less influence over ensuring the security of products and their information networks originating from third countries.

As a result of the Fourth Industrial Revolution, smart devices are becoming increasingly prevalent worldwide. The term "Fourth Industrial Revolution" is attributed to Klaus Schwab, who encapsulated it as follows:

> "The fourth industrial revolution, however, is not only about smart and connected machines and systems. Its scope is much wider. Occurring simultaneously are waves of further breakthroughs in areas ranging from gene sequencing to nanotechnology, from renewables to quantum computing. It is the fusion of these technologies and their interaction across the physical, digital and biological domains that make the fourth industrial revolution fundamentally different from previous revolutions."[2]

The Fourth Industrial Revolution has brought innovations that significantly influence all our lives, from smart home devices controlled by smartphones to smartwatches. As Csaba Krasznay points out, even a simple cable may contain microprocessors, the specific data processing of which we may not necessarily know. The existence of a "digital society" today indispensably involves surrounding ourselves with an increasing number of internet-connected devices. The risks and hazards associated with IoT (Internet of Things) devices, systems, and services are multifaceted, rapidly evolving, and encompass an extremely wide range of areas. Therefore, it is crucial to understand the theoretical frameworks and regulatory environments necessary for ensuring the security of such devices, as well as to develop operational measures to protect them from various threats. As highlighted by the European Union Agency for Cybersecurity (ENISA), the complexity of IoT devices poses a particular challenge.[3] In various reports, ENISA has underscored that the increasing complexity of IoT devices – due to their diverse functions, connectivity, and deployment environments – makes securing them particularly difficult. This complexity introduces a wide array of security and privacy risks, which are exacerbated by the rapid growth and innovation in IoT technology.

In parallel with the increasing prevalence of clean, sensor-based data-collecting smart devices, another significant trend unfolding in the 21st century is the escalating data collection processes by various governmental and non-governmental organisations. Globally, the terrorist attacks against the United States on 11 September 2001 marked a turning point wherein the significance of information derived from cyberspace was heightened. Following the clarification of the circumstances surrounding the globally shocking terrorist attacks, the United States gradually initiated its mass surveillance program, details of which were made public by Edward Snowden. Snowden and other, less-known activists and hacker groups pointed out regulatory deficiencies associated with the comprehensive program.[4]

[2] Schwab 2023.

[3] ENISA 2020; ENISA 2018.

[4] Deibert 2015; Snowden 2019.

In 2017, a document titled “Vault 7”, concerning hacker tools leaked by the CIA, was released by WikiLeaks. The description shed light on the organization actively seeking vulnerabilities in smart devices such as smartphones, smart TVs, and even passenger vehicles. Since modern passenger vehicles are particularly adept at collecting and transmitting large amounts of data, they may be suitable for a state to employ in coordinated covert information gathering. Given the increasing prevalence of electric passenger vehicles in the market due to their advancement and China’s notable technological advantage in this area, special attention should be paid to this aspect when developing regulatory frameworks.

The integration of Chinese electric passenger vehicles into the European market has been a subject of increasing interest and scrutiny in recent years. As these vehicles become more prevalent on European roads, concerns regarding the potential misuse of the data they collect and transmit have emerged. This study seeks to delve into the roots and processes behind the proliferation of Chinese electric passenger vehicles in Europe, while also exploring the associated information security challenges and national security risks.

Initially, we provide an overview of the emergence and expansion of Chinese electric passenger vehicles in the European market. Subsequently, we investigate the potential vulnerabilities inherent in the information transmitted by these vehicles, particularly focusing on how they can be exploited for covert surveillance, thus posing significant national security risks. Furthermore, this study highlights the efforts made by the European Union (EU) to enhance and refine its regulatory framework in response to the growing presence of internet-connected products, including electric passenger vehicles. By analysing recent EU directives and initiatives, we aim to assess the adequacy of existing regulations in addressing the information security threats posed by these vehicles.

To complement our analysis, we conducted interview-based research involving ten domestic experts familiar with the European regulatory landscape and automotive industry. Through these interviews, we sought to gain insights into the current state of the regulatory environment and its preparedness to address emerging challenges.

The primary objective of this study is to critically evaluate whether the regulatory environment of the European Union adequately addresses the information security challenges posed by the increasing presence of electric passenger vehicles in the market.

The origin of electric passenger vehicles from the People’s Republic of China

The Chinese government has encouraged the production and proliferation of electric vehicles through numerous market regulations and support programs. For instance, vehicle manufacturers were obligated to meet mandatory quotas for the sale of electric vehicles, which facilitated the industry’s growth. Additionally, they were provided with tax incentives, purchase subsidies, and state support for the establishment of charging infrastructure.

China’s national industrialisation and commercialisation of electric vehicles began in early 2009. Through the provision of financial support, it gradually progressed from initiatives in public transportation to those in private consumption, from urbanisation experiments to regional trials, and finally to national-level promotion. The aim of this multifaceted, step-by-step policy was to stimulate investment, promote industrial growth, and alleviate the challenges of the initial phase. Simultaneously, the subsidies were planned to be phased out gradually, and the eligibility thresholds, characteristic of their accessibility, were to be raised progressively. This required the establishment of industrial clusters with global competitiveness. The support policies had to undergo three different stages of modification to facilitate industrial development.

In the "12th Five-Year Plan for the Development of Electric Vehicles" issued in 2012, China officially proposed the implementation of a phased strategy for the industrialisation of electric vehicles, dividing the process into three phases. The first phase took place from 2009 to 2012; the second phase from 2013 to 2015, and the third phase from 2016 to 2020.[5] In 2010, the State Council issued the "Decision on Accelerating the Development of Strategic Emerging Industries", which classified the electric vehicle industry, the energy efficiency industry, the environmental protection industry, and other related sectors as strategic emerging industries in China.[6] Strategic emerging industries are considered sectors with significant technological innovation potential that are in the early stages of development. It is evident that studying national-level political incentives and influences holds both theoretical and practical significance. The electric vehicle industry serves as a typical example of strategic emerging industries in China, playing a prominent role in steering China's economic and technological development over the past decade.[7] Since then, thanks to related programs and policies, the industry has made significant progress and is currently in the stage of technical and commercial demonstration.

In China's transportation sector, energy consumption has increased by nearly 10% annually, accounting for nearly 15% of total energy consumption. In 2019, the national vehicle fleet reached 348 million, representing a 6.4% increase over the previous year. Among them, the number of "new energy vehicles" (NEVs) reached 3.81 million. The total emissions of the four evaluated pollutants from national vehicles amounted to 16,038 kt; CO_2 emissions from gasoline vehicles exceeded 80% of total vehicle emissions, and HC emissions exceeded the pollution threshold by 70%, according to the Annual Report of the Chinese Transportation Source Environmental Management.[8]

In response to these challenges, the Chinese government launched two environmentally friendly NEV demonstration projects to promote the commercial utilisation of vehicles. The first phase ran from January 2009 to December 2012, covering 25 pilot cities including Beijing, Shanghai, Hangzhou, Dalian, and Shenzhen. Initially, the demonstration project focused on public areas (such as buses and special vehicles), then expanded to private areas starting from May 2010. However, the results of the first phase fell short of expectations. Consequently, the Chinese government issued a statement titled "Continued Work to Promote the Development of New Energy Vehicles", deciding to continue the demonstration

[5] Wu et al. 2021.

[6] The Central People's Government of the People's Republic of China 2010.

[7] Zhang et al. 2017.

[8] China Mobile Limited 2020.

project for the next three years, known as the second phase NEV demonstration project. The second phase project encompassed 39 cities (urban groups), totalling 88 cities.[9]

Based on the above, it becomes clear that the Chinese electric vehicle industry has been active for at least a decade and has shown significant progress. Although the increased production for export and the prioritisation of the European Union as a market have only occurred in the last few years, it could have been anticipated with proper attention to market expansion, and accordingly, a stricter regulatory environment could have been established.

The data transmission mechanisms of passenger vehicles and the preparedness of the European Union

In the past decade, the European Union has issued numerous regulations, best practices, and guidelines aimed at enhancing the security of digital devices used by consumers. In recent years, data protection has increasingly featured prominently in the listed standards, which will be elaborated upon in the following section. The most significant development in terms of regulatory environment in recent years has been the introduction of the NIS2 regulation, which member states are obliged to transpose into national legislation. Since NIS2 applies not only to governmental but also to a wide range of market players, including suppliers, it represents a significant advancement in the field of data security. However, it can be asserted that in terms of requirements, it does not present a sufficiently modern solution, as it is largely based on the NIST 800-53 r5 standard, which is a generic, organisation-focused information security standard and does not specifically consider the safety of products used by consumers, nor was it created for this purpose.

Although, the role of data security is increasingly emphasised in new regulations, it can also be observed that among the regulations, only the GDPR focuses specifically on consumer data and the transparency of data flow. The aim of this study is not to comprehensively present the problems related to the GDPR, but below, we have collected some examples to illustrate that despite the application of the GDPR, several challenges still arise, and compliance alone does not guarantee that users can be informed about the use of their data (examples 1, 2, 3, 4). It is also important to note that regulations related to various cloud services and a series of regulations concerning industrial devices are relevant to the topic of this study due to network communication; however, these are not discussed in this research due to limitations of scope.

The data processing of personal information related to connected cars is governed by data protection guidelines, which sometimes link loosely defined and/or incompatible purposes (e.g. providing requested services, credit and behaviour assessment, and operating and expanding business activities). For example, data originally collected for maintenance purposes can be used by insurance companies to enrich driver profiles, develop individual pricing, offer insurance policies based on driving behaviour, or investigate liability in car accidents. Traffic safety authorities could use this data to enforce traffic rules, such

[9] Wang et al. 2017.

as speed limit enforcement. Every piece of data related to a person's car use, such as driving routes and destinations, in-car communications, or infotainment services, can reveal sensitive information about the individual's life. People's driving habits and places of interest can not only enable their identification, but also infer sensitive information such as religious and political affiliations, sexual orientation, and relationships. Therefore, the collected data is useful for profiling and monitoring individuals, especially when it is linked to existing (private or governmental) databases. Data controllers must pay particular attention to the requirements imposed by the GDPR on the processing of special categories of data, such as the limited available legal bases. Data controllers must clearly inform users of connected cars about the purpose of processing location data. Due to the sensitive nature of location data, the thorough application of data protection principles, especially purpose limitation, data minimisation, and data storage, is necessary.

Although various standards and regulations applied in the automotive industry now also encompass supply chain protection, which often means suppliers complying with standards equivalent to those of manufacturers, information security standards generally provide a framework rather than specific instructions regarding conditions. This is necessary, because certain degrees of flexibility are crucial due to different specialised situations.

In 2007, Gunnar Peterson and Elizabeth Nichols introduced metrics to measure how changes in processes during a given lifecycle can affect security in the next phase. Accordingly, they developed various metrics and examined their applicability, also focusing on monitoring system availability, reliability, and maintainability.[10] In 2008, Dan and Julie Ryan conducted a study on security and data privacy, exploring how ineffective risk measures could be enhanced and better adapted to reality. They also developed impact analysis related to investments in information security and tracking changes in expected losses.[11] In 2010, Cunningham and Pfleeger (2010) published a report on nine "compelling reasons" explaining why measuring security is difficult.[12] Later, David Evans, Steve Bellovin, and Sal Stolfo (2011) published an article discussing the use of science-based, systematic and generalised knowledge, the development of universal principles for forecasting, and the use of methodologies for testing hypotheses as tools for anecdote-driven security decision-making.[13] In 2012, George Cybenko and Carl Landwehr (2012) prepared a study on the necessity of measuring security progress. Cybenko elaborated on the difficulty of demonstrating progress in operational cybersecurity, while Landwehr wrote about the need to improve the reliable measurement of cybersecurity status at national and international levels, advocating for measurements to be controlled by an unbiased organisation.[14] They discussed past mistakes and how the game-theoretic application of illegal usage can be misleading. The authors also wrote about the lessons learned from observing the gradual increase in risk and the fluctuating nature of these types

[10] Nichols–Peterson 2007.

[11] Ryan–Ryan 2008.

[12] Pfleeger–Cunningham 2010.

[13] Stolfo et al. 2011.

[14] Cybenko–Landwehr 2012.

of data.[15] Omoyiola's research (2020) aims to review previous research on information security measurement and testing and summarises developments in the field over the past years. According to the research, the field of information security measurement and testing is dynamically evolving, introducing numerous new methods and tools in recent decades to assess and improve security levels. The study reviews various methods of information security measurement and testing, such as signature analysis, vulnerability scanning, penetration testing, simulations, model-based testing, and hybrid methods. The study emphasises that information security measurement and testing remain crucial for improving security levels and maintaining information security, and these activities must evolve dynamically in response to security threats.[16]

The above enumeration highlights a complex, continually evolving field, of which data protection and transparency constitute only a small part. In recent years, particularly following the introduction of the GDPR, chapters addressing data protection have emerged in standards, providing practical guidance on how standard adopters should proceed concerning their clients or other individuals. A prime example of this evolution is the difference between NIST 800-53 r4 (originally released in 2014)[17] and NIST 800-53 r5 (originally released in 2020),[18] wherein, among other changes, the 2020 standard introduces a new control family specifically addressing data protection.

Passenger vehicles and data security incidents

Modern vehicles contain interconnected electronic systems that can be potential targets for various threatening actors present in cyberspace. Today's cars can interact with their environment by exchanging data with control stations that provide a wide range of services to urban populations. This connectivity extends beyond smart cities to include connections with telecommunication networks. Additionally, vehicles incorporate sophisticated controllers that manage data collected in real-time through sensor networks. As a result, they play a similar role in cyberspace as mobile phones or computers. This connectivity enables functions such as emergency calls (eCall) and accessing entertainment and other content through online connectivity while traveling. Additionally, besides over-the-air (OTA) services, it provides software updates for digital content in the vehicle.[19]

To enable the manufacturer to send over-the-air (OTA) updates to the entertainment electronics devices in the vehicle, it is necessary to ensure that software remains up-to-date without requiring the owner to visit a service centre. This functionality not only provides convenience, but also proves useful for promptly addressing security vulnerabilities. However, since vehicles communicate over simple HTTPS protocols similar to mobile phones, they are exposed to various vulnerabilities.

[15] Pfleeger 2012.

[16] Omoyiola 2020.

[17] See: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2014-01-15

[18] See: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[19] Venkat 2020.

In 2016, a group of Chinese security researchers from the Keen Security Lab discovered a method to breach the Controller Area Network (CAN) bus found in Tesla models, which controls displays and brakes.[20] The researchers were able to remotely access the central control unit and adjust the mirrors, lock the doors, manipulate the dashboard, and even activate the brakes. This was reported to Tesla, and the company responded to the disclosure with a newly issued update. However, this event clearly highlighted the problem of using outdated software. Several years later, another team from the Keen Security Lab discovered 14 vulnerabilities in vehicles manufactured by BMW.[21]

The data collected and transmitted in this manner not only facilitate economic crimes but are also suitable for clandestine surveillance conducted by state entities. In a previous study from 2023, we illustrated through the development of a theoretical model that such surveillance, employing multiple vehicles, could potentially encompass an individual's entire daily activities outside of an office building.[22]

Interview-based research: the state of data security in the automotive industry according to domestic experts

The research methodology chosen for this study is in-depth interviewing, considering the sensitive nature and complexity of the topic. The distinct feature of in-depth interviewing is that the researcher engages in dialogue with the interviewees based on predefined topics rather than a set question list, aiming to gather contextual information that may not have emerged from preliminary research.[23] While in-depth interviews are not suitable for generalising findings, they provide an opportunity to gather and summarise the experiences and recommendations of experts deeply knowledgeable in the field.

For this study, a semi-structured interviewing method falling within the category of field research was selected to conduct the research, as it aligns with the subject matter.[24] The aim of the empirical research is twofold: firstly, to understand the opinions of Hungarian experts on the data security issues raised in the study, and secondly, to gather proposed solutions to the challenges identified. Since this approach requires deeper dialogue and cannot be addressed simply through, for example, a questionnaire method, the use of in-depth interviews is justified. The interviews were conducted in an open-ended manner, allowing for interactive discussions beyond the initial questions and responses, which facilitated the acquisition of additional information.[25] During the interviews, it was important to uncover new information that did not arise during the literature review but could form the basis for further investigation.

To determine the appropriate questions, three dimensions were delineated based on the topics covered in the thesis: challenges related to data security in automobiles, consumer

[20] Perrig et al. 2002.

[21] Zorz 2018.

[22] Hegyi–Erdődi 2023.

[23] Babbie 2020.

[24] Babbie 2020.

[25] Babbie 2020.

responsibility and awareness, and potential solutions. These dimensions were ordered from broader to more specific to ensure clarity regarding the general approach used by the selected experts in their work and to identify any specific issues related to automotive information security.

Since not all experts possess the same depth of experience in the automotive industry, but may still have relevant professional insights applicable to the sector, it was important that industry-specific questions were used only to gather supplementary information. These questions were asked only if the interviewee had actual experience in this area.

Narrative analysis

In order to examine the practical difficulties of implementing information security standards, it was necessary to analyse the information generated during the interviews using a technique that allows for more than just isolated facts to be determined.[26] Regarding the auditing work and standards, deeper underlying reasons for differences between theory and practice, or subjective factors influencing the results, can be identified. The interview transcripts were analysed using the Krippendorff content analysis methodology, which emphasises that context is an integral part of text analysis. This approach aligns with the complex nature of the study by allowing the researcher to draw inductive conclusions about the content.[27]

Sampling

The central subjects of the qualitative, in-depth interview-based research are information security experts, including auditors, consultants, and researchers. However, to uncover relevant information during the analysis, it was necessary to narrow down the initial group of 30 participants. During the selection of the 10 interviewees for the research, a filtering criterion was applied, requiring a minimum of 5 years of work experience in one of the information security professions (seniority), as well as expertise gained in at least 5 different industries or areas. These criteria ensure that the experts possess sufficiently broad practical knowledge regarding the researched questions. Experience in the automotive industry was not a requirement, as deep sectoral knowledge is not necessary to answer the research questions, but a wide-ranging understanding of the regulatory environment in various industries facilitates the recognition of best practices.

As a result, the sample included, for example, a professional mainly working with Hungarian small and medium-sized enterprises (SMEs), as well as one currently employed in the public sector, with previous clients and employers including financial institutions, pharmaceutical factories, and food industry companies.

[26] Babbie 2020.

[27] Krippendorf 2018.

Results

From the responses of the interviewees, it is apparent that five respondents have worked on information security projects or tasks related to the automotive industry, while the other five individuals do not have such experience. Therefore, industry-specific questions related to automotive standards were only asked to the former group of five individuals.

Regarding the challenges, several interviewees highlighted the complexity of vehicles as end products. Two interviewees also pointed out that supporting the software environment of personal vehicles is becoming increasingly challenging. If software support expires, adequate protection is no longer guaranteed. From a cybersecurity perspective, it is considered a challenge that users do not have visibility into what exactly happens with the car's IT system and data during a service. Some interviewees suggested that this should be ensured not only through proper information but also through dedicated archival tools, essentially requiring a black box, similar to those used in aviation.

One of the interviewees pointed out that broader application of the Common Criteria standard could provide a solution for taking a product-based approach to information security in passenger vehicles.[28] However, upon reviewing the list of certified devices on the standard's official website, it becomes apparent that only a few devices worldwide have this certification. Moreover, the majority of these devices are general-purpose IT tools, such as firewalls.

When it comes to the ISO/IEC 21434 standard, we are indeed dealing with an industry-specific standard, but the examination object is not the vehicle itself; rather, it focuses on certain electronic components of the vehicle. These components could include, for example, the electronic parts controlling the brakes or the Bluetooth module of an infotainment system. From the perspective of vehicle security, it is problematic that certification is not expected for every component, which means that its impact only applies "patchily" depending on the manufacturer's requirements. This situation arises not only from a managerial perspective but also from limited resources, as compliance with strict regulations can incur high costs.

Regarding comprehensive solutions, nearly every expert agreed that there is a need for a unified European-level legislation that precisely dictates the application of controls to vehicle manufacturers and suppliers, which are currently included in standards. Associated with this is the necessity to establish an authority to enforce these rules. One interviewee also pointed out that as long as economic factors do not incentivise manufacturers for greater diligence, the situation will remain unchanged.

Finally, out of the ten interviewees, three mentioned increasing user awareness as a proposed solution. According to the general opinion of the interviewees, users are generally not interested in information security issues, unless a device malfunctions or their data is genuinely at risk of being compromised or leaked.

In connection with this, diverse solutions have been proposed, ranging from general education in primary schools (such as information security lectures during computer classes) to providing more transparent informational texts.

[28] See: https://www.commoncriteriaportal.org/products

There was also an opinion suggesting that advanced convenience and service-oriented features and practices, such as providing seat heating as a service, should be banned concerning vehicles. The logical background of this idea is that the development of information technology has reached such proportions today that security experts and standards cannot keep pace with it in any way.

Summary

In this study, we first presented the roots and processes of the spread of Chinese electric passenger vehicles in the European market. In the following chapters, we explored the potential problems caused by the malicious use of information transmitted by passenger vehicles and discussed how vehicles can be used for covert surveillance, posing national security risks. We also showcased the steps taken by the European Union in recent years to improve and develop the regulatory environment.

Through the interview-based research conducted with the assistance of ten domestic experts, we concluded that the regulatory environment of the European Union is not prepared to handle the threat posed by the mass influx of internet-connected products, namely electric passenger vehicles, originating from third countries.

Among the proposed solutions, there was roughly equal emphasis on raising awareness among users and increasing their sense of responsibility, although there was an opinion suggesting this is unnecessary. According to this viewpoint, consumers should not be entrusted with the protection of their data, as it cannot be ruled out that they may lack the necessary knowledge and preparedness for this task. Another proposed solution was the designation of a European Union-level authority capable of providing expert advice at a higher level on contentious issues related to information security and data protection and acting as a regulatory authority against abuses and omissions.

The purpose of the study was to examine whether the regulatory environment of the European Union is adequate to combat the information security challenges posed by the large volume of electric passenger vehicles currently entering the market. Based on the literature review and interviews, it can be concluded that it is not. However, further research is advisable to examine the proposed solutions and develop additional ones.

References

Babbie, Earl (2020): *A társadalomtudományi kutatás gyakorlata.* Budapest: Balassi.

China Mobile Limited (2020): *Digitalized and Intelligent New Power for All.* China Mobile Limited Sustainability Report. Online: https://www.chinamobileltd.com/en/ir/reports/ar2020/sd2020.pdf

Cybenko, George – Landwehr, Carl (2012): Security Analytics and Measurements. *IEEE Security & Privacy,* 10(3), 5–8. Online: https://doi.org/10.1109/MSP.2012.75

Deibert, Ron (2015): The Geopolitics of Cyberspace after Snowden. *Current History*, 114(768), 9–15. Online: https://doi.org/10.1525/curh.2015.114.768.9

European Union Agency for Cybersecurity (ENISA) (2018): *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing.* 19 November 2018. Online: https://doi.org/10.2824/851384

European Union Agency for Cybersecurity (ENISA) (2020): *Guidelines for Securing the Internet of Things*. 9 November 2020. Online: https://doi.org/10.2824/314452

Hegyi, Henrietta – Erdődi, László (2023): Személygépjárművek adatforgalmának megfigyelési célú felhasználási lehetőségei. *Biztonságtudományi Szemle*, 5(1), 53–67.

Krippendorff, Klaus (2018): *Content Analysis. An Introduction to Its Methodology.* Thousand Oaks: SAGE. Online: https://doi.org/10.4135/9781071878781

Nichols, Elizabeth A. – Peterson, Gunnar (2007): A Metrics Framework to Drive Application Security Improvement. *IEEE Security & Privacy*, 5(2), 88–91. Online: https://doi.org/10.1109/MSP.2007.26

Omoyiola, Bayo Olushola (2020): The Evolution of Information Security Measurement and Testing. *IOSR Journal of Computer Engineering*, 22(3), 50–54. Online: http://dx.doi.org/10.9790/0661-2203025054

Perrig, Adrian – Canetti, Ran – Tyar, J. D. – Song, Dawn (2002): The Tesla Broadcast Authentication Protocol. *CryptoBytes*, 5(2), 2–13.

Pfleeger, Shari L. (2012): Security Measurement Steps, Missteps, and Next Steps. *IEEE Security & Privacy*, 10(4), 5–9. Online: https://doi.org/10.1109/MSP.2012.106

Pfleeger, Shari L. – Cunningham, Robert (2010): Why Measuring Security Is Hard. *IEEE Security & Privacy*, 8(4), 46–54. Online: https://doi.org/10.1109/MSP.2010.60

Ryan, J. C. H. – Ryan, D. J. (2008): Performance Metrics for Information Security Risk Management. *IEEE Security & Privacy*, 6(5), 38–44. Online: https://doi.org/10.1109/MSP.2008.125

Schwab, Klaus (2023): The Fourth Industrial Revolution. *Encyclopedia Britannica*, 31 May 2023. Online: https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734

Snowden, Edward (2019): *Rendszerhiba*. Trans. Tomori Gábor. Budapest: XXI. Század.

Stolfo, Salvatore – Bellovin, Steven M. – Evans, David (2011): Measuring Security. *IEEE Security & Privacy*, 9(3), 60–65. Online: https://doi.org/10.1109/MSP.2011.56

The Central People’s Government of the People’s Republic of China (2010): *Decision on Accelerating the Cultivation and Development of Strategic Emerging Industries Released in October 2010.* Online: http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm

Venkat, Subbu (2020): *Evolving Automotive Gateways for Next-Generation Vehicles*, Texas Instruments. Online: https://www.ti.com/lit/wp/spry333b/spry333b.pdf?ts=1712501484924

Wang, Ning – Pan, Huizhong – Zheng, Wenhui (2017): Assessment of the Incentives on Electric Vehicle Promotion in China. *Transportation Research Part A: Policy and Practice*, 101, 177–189. Online: https://doi.org/10.1016/j.tra.2017.04.037

Wu, Yang Andrew – Ng, Artie W. – Yu, Zichao – Huang, Jie – Meng, Ke – Dong, Z. Y. (2021): A Review of Evolutionary Policy Incentives for Sustainable Development of Electric Vehicles in China: Strategic Implications. *Energy Policy*, 148. Online: https://doi.org/10.1016/j.enpol.2020.111983

ZHANG, Xingping – LIANG, Yanni – YU, Enhai – JIAN XIE, Rao Rao (2017): Review of Electric Vehicle Policies in China: Content Summary and Effect Analysis. *Renewable and Sustainable Energy Reviews*, 70, 698–714. Online: https://doi.org/10.1016/j.rser.2016.11.250

ZORZ, Zeljka (2018): Researchers Hack BMW Cars, Discover 14 Vulnerabilities. *Help Net Security*, 23 May 2018. Online: https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/