Potential risks of using Advanced Driver Assistance Systems (ADAS) on Wuling Almaz as a media for Chinese espionage in Indonesia

Bagus Tri Wibowo[1], Diky Zakaria[2,*], Armi Susandi[3], Maya Rahayu[4], Md. Biplob Hossain[5], Tajul Miftahushudur[6]

[1] Program Studi Agen Intelijen, Sekolah Tinggi Intelijen Negara, Bogor, Indonesia
[2] Program Studi Mekatronika dan Kecerdasan Buatan, Universitas Pendidikan Indonesia, Bandung, Indonesia
[3] Institut Teknologi Bandung, Bandung, Indonesia
[4] Okayama University, Okayama, Japan
[5] Electrical and Electronic Engineering Department, Khwaja Yunus Ali University, Bangladesh
[6] Department of Electrical & Electronic Engineering, The University of Manchester, Manchester, United Kingdom

Article history
Received: 12 April 2025
Revised: 23 April 2025
Accepted: 26 April 2025

Keywords
Advanced Driver Assistance Systems (ADAS)
Chinese Espionage
Wuling Almaz

Abstract
The utilization of internet of vehicle technologies such as driving assistance technology brings up numerous system risks and information leakage. In the future, if vehicle technology is not properly managed, the misuse of driving assistance technology could occur, perhaps leading to the collection of national strategic information. Indonesia's vast human resources have enticed global corporations to establish themselves in the country as suppliers for Southeast Asia. This issue has prompted experts to recognize the imperative need for enhancements in intelligence, specifically by the National Intelligence Agency (BIN), in order to prevent the potential exploitation by both domestic and international actors. The problem at hand concerns the possibility of ADAS being used for espionage purposes and the resulting consequences for national security. The research utilizes a descriptive qualitative methodology that draws upon theories related to espionage, intelligence, threats, data breach/information theft, and surveillance tactics. The findings suggest that while intelligence and cybersecurity experts recognize the potential risks associated with driving assistance technology, those directly involved in the academic and industry sectors have not yet acknowledged these advancements. The lack of preparedness of Indonesian society and government in dealing with technology improvements in the automotive sector worsens this issue. Hence, intelligence authorities deem it imperative to engage in thorough deliberations over Indonesia's approach to mitigate potential espionage risks arising from the advancement of driving assistance technologies.

1. Introduction

Advanced Driver Assistance Systems (ADAS) encompass both established and emerging in-vehicle technology systems that are specifically designed to aid the driver in performing the driving duty (Nandavar et al., 2023). This technology offers vital data regarding traffic conditions, road closures, obstructions ahead, levels of congestion, and suggested alternative routes to circumvent traffic congestion. ADAS has the capability to assume control from humans in evaluating potential dangers, carrying out basic functions such as maintaining a constant speed, or executing intricate actions like passing other vehicles and parking. An inherent benefit of utilizing this support system is its ability to facilitate communication across diverse cars, vehicle infrastructure systems, and transportation management centers for the purposes of vehicle localization, planning, and decision-making (Azevedo & Santos, 2024; Wood et al., 2024). ADAS employs a diverse range of sensors, cameras, radar, and other technologies to aid drivers in various scenarios. Several automobile manufacturers, including Tesla, Mercedes-Benz, BMW, Audi, Toyota, Honda, and Wuling have implemented ADAS in their product.

In relation to the Wuling brand, the Wuling Almaz type has implemented ADAS technology which uses sensors and camera technology, radar, Light and Ranging (LiDAR) and computer vision. The integration of various sensors allows the Almaz type Wuling car to operate at level three autonomous vehicle, namely this

*Diky Zakaria, email: dikyzak@upi.edu

car is able to activate features such as adaptive cruise control, lane keep assist, safe distance warning, and forward collision warning (Wuling, 2022). Automobile manufacturers, include Wuling are increasingly installing cameras and sensors in vehicles to collect photos of the car's surrounds. However, the control over the usage, destination, and storage of these photos is becoming a pressing concern for both the industry and regulators worldwide. Tesla automobiles are banned by the Chinese military complex due to concerns about their ability to compromise security and facilitate espionage (Reuters, 2021). In addition, Joe Biden initiated an investigation into connected vehicle (CV) that originate from China due to their ability to gather and transmit significant data, such as position, images/videos of the surrounding environment, and other crucial information (Whalen, 2024). In January 2023, a Chinese tracking device was discovered in a car belonging to the UK government, leading to the conclusion that it posed a significant and organized security risk (Madeleine, 2023). In addition, car manufacturers often establish non-negotiable customer agreements, which pose challenges for consumers in securing their privacy (Pesé et al., 2020).

Based on this description, it appears that the utilization of ADAS technology in the Wuling Almaz automobile has the potential to facilitate espionage. Indonesia and China engage in extensive collaboration across diverse domains, including economics and technology. From an intelligence point of view, it is necessary to evaluate, analyze, and interpret the possibility of espionage in order to give advance notice and anticipates potential dangers to national security. This paper aim to investigate the potential threat posed by the Advanced Driver Assistance System (ADAS) in Almaz-type Wuling vehicles for espionage activities in Indonesia and to explore mitigation efforts to counteract this threat, which is the originality of this paper. In order to accomplish the research objectives, we did a thorough review of relevant literature and conducted interviews with relevant stakeholders and experts.

2. Literature Review

2.1. Advance Driver Assistance System (ADAS)

ADAS, or Advanced Driver Assistance Systems, is an advanced technology integrated into vehicles that provides assistance to the primary driver in multiple ways. This technology can be utilized to deliver crucial data like traffic conditions, road closures, obstructions ahead, levels of congestion, recommended alternative routes to circumvent traffic congestion, and similar information (DeGuzman & Donmez, 2022; Wood et al., 2024). The system has the ability to assume control from humans in evaluating any potential danger, doing simple tasks like maintaining a constant speed or executing complex movements such as changing lanes and parking. An important benefit of utilizing this support system is its ability to facilitate communication across different cars, vehicle infrastructure systems, and transportation management centers responsible for vehicle localization, planning, and decision-making.

ADAS systems encompass a collection of automotive technologies and features specifically developed to enhance the safety and convenience of drivers and passengers in cars. ADAS employs a diverse range of sensors, hardware, and software to actively observe and react to the immediate environment of the vehicle. The inclusion of advanced features such as adaptive speed control, in-lane driver assistant, blind spot detection, emergency automatic braking, cross-traffic monitoring, traffic sign recognition, parking assistant, and various others significantly enhance driver safety by assisting in potentially hazardous circumstances (Nandavar et al., 2023; Wood et al., 2024). The primary objective of this system is to mitigate the likelihood of accidents, minimize driver tiredness, and enhance the overall safety and comfort of the driving experience. While ADAS features can assist drivers, it is crucial for drivers to maintain attention and accountability while driving, as this system serves as a supplementary tool rather than a substitute for the driver.

2.2. Data Breach / Information Theft

Information theft encompasses a series of actions that involve the unlawful access or acquisition of confidential data, sensitive information, or valuable items belonging to an individual, company, or other entity. This phenomena is interconnected with cyber security and information security and serves as a prominent subject in the continuously expanding digital landscape (Khan et al., 2020). Information theft can be perpetrated through several methods, such as computer hacking, cyber-attacks, phishing, physical theft, unauthorized access by inside personnel, or snooping. Individuals that engage in information theft may have several motivations, such as financial, competitive, political, or criminal reasons. They may have the intention to pilfer information in order to acquire monetary benefits, obtain a competitive edge, secure political advantages, or pose a threat to national security. Information theft can have a highly damaging consequence (Sarker et al., 2020). Potential consequences of a cyber-attack include monetary damages for individuals or organizations, erosion of customer confidence, breaches of privacy, and even risks to national security when dealing with sensitive information.

2.3. Surveillance Technique

The term "surveillance" refers to the systematic observation or monitoring of particular activities, behaviors, or information with the intention of achieving a particular objective (Saheb, 2023). The collection, documentation, and analysis of pertinent data can be performed through the use of a variety of approaches and technologies to carry out surveillance. The reasons for conducting surveillance may include ensuring safety, keeping an eye on people's health, or gathering information for the purpose of achieving commercial or government objectives (Ogasawara, 2022).

2.4. Intelligence Theory

The Republic of Indonesia Law Number 17 of 2011, specifically in article 1 paragraph 1, defines intelligence as the acquisition of knowledge, the establishment of organizations, and the execution of activities that pertain to the development of policies, national strategies, and decision-making processes. This is done through the analysis of information and facts gathered using specific methods for detection and early warning, with the ultimate goal of preventing, deterring, and addressing any potential threats to national security. According to the given legislative definition, intelligence is closely linked to national security and is seen as a method for preventing, discouraging, and addressing any risks to national interests. Intelligence refers to highly pertinent information and analysis that directly relates to the president's interests and obligations as the leader of the nation. Intelligence is gathered through covert operations, which are crucial but not the sole aspect of obtaining information. Covert operations are employed to gather intelligence from confidential sources, yet they are not conducted on a tiny scale and are utilized to comprehend the intricacies of real strategic matters (Russell, 2007).

2.5. Espionage Theory

Espionage refers to the deliberate gathering of secret information by one party from another party. Perpetrators of espionage can encompass individuals, collectives, or governmental entities. Intelligence gathered through espionage can be utilized for strategic, military, economic, political, or competitive objectives (Hou & Wang, 2020; Phillips & Pohl, 2024). Espionage can be categorized as a covert operation that involves the clandestine acquisition of information, often employing advanced technology. Moreover, espionage technology include tools that streamline the information gathering process, including monitoring devices, both in the form of software and hardware (Wallace et al., 2009).

3. Method

3.1. Data Source

The research questions of this study are as follows:

a. What is the possible risk posed by the advanced driver assistance system on Almaz type Wuling vehicles for espionage actions aimed at gathering strategic information in Indonesia?

b. What actions are being taken to address the potential risk of the advanced driver assistance system on the Wuling Almaz type being used for espionage activities to obtain strategic information in Indonesia?

In order to address these two research questions, we applied a descriptive qualitative approach that was modified from Chiu et al. (2024) and Zou et al. (2024).

3.2. Ethical Considerations

Before the interview was carried out, each and every sourceperson was given a detailed explanation of the purpose, the significance of the issue, the procedures, and the confidentiality of the information. In the presentation that is contained inside this article, the full names of each individual sourceperson will not be mentioned here. To ensure that the sourceperson's information remains private, this step has been put into place. A communication has been sent to the sourceperson informing them that any information they supply will be used for the purposes of this research project. In the event that there is any information that is regarded to be inappropriate, the sourceperson who gave the information retains the right to retract the information at any time.

3.3. Data Collection

Data collecting procedures are the specific strategies employed to gather or acquire data in a research investigation. This study will utilize interview approaches as a way of collecting data. An interview is a method of communication or discourse in which a researcher poses questions to a resource person, who then delivers responses. The interview method employed is a semi-structured interview. We did the semi-structured in-depth interview with the 6 experts (sourceperson) from different stakeholders such as state intelligence agency, national cyber crypto agency, Indonesia cyber security forum, Wuling sales consultant, cyber security practitioner, mechatronics and artificial intelligence expert. The semi-structured interview guide can be seen in Table 1.

Table 1. Guidance for semi-structured interview.

Question for	Questions
State intelligence agency and national cyber crypto agency	• What is the extent of oversight by the state intelligence agency about Wuling automobiles imported from China? • What is your opinion on the Wuling vehicle that is equipped with an Advanced Driver Assistance System (ADAS)? • How does the state intelligence agency identify potential espionage risks associated with Wuling automobiles equipped with the ADAS system? • What are the necessary requirements to allow Wuling to maintain the use of the ADAS system? • Does the possible risk of espionage via the ADAS system significantly affect Indonesia's security? • Do you believe that the Chinese government engages in any form of intervention in ADAS if it is utilized as a means of conducting espionage? • What measures have state intelligence agencies taken to address the issue of automobiles incorporating ADAS systems? • How does the state intelligence agency offer feedback and recommendations to the Government concerning this matter? • Which Intelligence Strategy may be employed to address potential espionage risks posed by ADAS systems on vehicles?
Indonesia cyber security forum, Wuling sales consultant, cyber security practitioner, mechatronics and artificial intelligence expert	• What are your views on rules related to autonomous vehicles? • In what ways might automobiles equip with ADAS technology function as tools for collecting information? • Does this phenomenon impact driving safety? • Can the ADAS system in vehicles be exploited for information theft? • What are the specific legislation governing the implementation of the Advanced Driver Assistance Systems (ADAS) on automobiles in Indonesia?

3.4. Data Analysis

Researchers employed qualitative data analysis methodologies to conduct information analysis in this study. Qualitative data analysis involves systematically searching and organizing data from various sources such as processed primary data, field reports, documentation, and literature studies. The collected data is then carefully arranged and described in detail, synthesizing the information. This analysis aims to identify the key elements that address the research problem and draw conclusions that are accessible to the general public.

3.5. Intelligence Analysis

Using a variety of methods, intelligence analysis is a socio-cognitive process that takes place within a secret domain. The goal of this process is to reduce a complicated issue to a group of smaller ones (Blanchard & Taddeo, 2023). The researchers will employ intelligence analysis utilizing the model set out by Soepono Soegirman (Soegirman, 2009), which possesses unique attributes and qualities in delivering judgment, forecasting, early warnings and problem solving based on the principles of proportionality, precision, and information correctness. In addition, intelligence analysis also takes into account problem solving when making conclusions concerning occurring phenomena. **Judgment** is the act of evaluating a case or circumstance in terms of its significance and assigning significance to it. Prediction, also known as **forecasting**, is the act of creating a prediction or estimate in order to decrease the amount of ambiguity regarding future events. This allows policy makers or users to utilize the prediction as a factor when making decisions. **Early warning** is a method of predicting outcomes that is utilized to provide advance notice of impending risks.

4. Results and Discussion

Individual interviews were done for each expert. The subsequent section presents the outcomes and analysis of the conducted interviews.

4.1. Potential Risks of the ADAS on Wuling Almaz in Collecting Information for Espionage Actions

ADAS functions by integrating a combination of sensors, cameras, and data processing systems to offer support to drivers and enhance the safety of driving. ADAS systems often incorporate a range of sensors including radar, LiDAR, ultrasonic, and cameras. These sensors are strategically positioned throughout the vehicle to accurately perceive the surrounding environment. Radar, LiDAR, and camera sensors gather data regarding the surrounding conditions of the vehicle (Qin et al., 2022; Seacrist et al., 2021). This encompasses data regarding the presence and positioning of vehicles in the vicinity, as well as road markings, pedestrians, vehicle license plate numbers, and other objects. This information is gathered through the utilization of radar, LiDAR, and camera sensors, which are then analyzed by data processing units situated within the vehicle. This processor employs intelligent algorithms to analyze data and discern potential scenarios that necessitate a response, thereby enabling vehicles equipped with ADAS to detect objects in their path, identify passing lanes, detect blind spots, adjust braking and acceleration, issue warnings about potential collisions, recognize driver characteristics, determine vehicle location, and facilitate software updates.

The vehicle is equipped with an electronic control unit that efficiently manages the input and output functions of the vehicle. When a vehicle system is equipped with Internet of Things (IoT) or Internet of Vehicles (IoV), it means that the vehicle is equipped with its own artificial intelligence through a computer system (Ji et al., 2020). This computer system is integrated into the entertainment unit located on the dashboard of the Wuling Almaz vehicle. Artificial intelligence in automobiles serves two purposes: enhancing system performance and addressing potential risks, such as the possibility of unintended espionage vulnerabilities resulting from information leaks over the internet of vehicles in Wuling Almaz vehicles. This aligns with the findings of McCall et al (2021) research, which indicate that the utilization of IoT and IoV can enhance the susceptibility to cyber-attacks.

To determine the potential of utilizing Advance Driver Assistance System (ADAS) technology, one must consider various factors such as data security vulnerabilities, the utilization of radar, LiDAR, and cameras positioned on all sides of the Wuling Almaz vehicle to provide a complete 360-degree view, the user-friendliness of operating Wuling Almaz vehicles through the MyWulingPlus application, and the presence of internet connectivity known as the Wuling Interconnected Smart Ecosystem (WISE) in Wuling Almaz vehicles. The Wuling Almaz vehicle is equipped with a microphone sensor that enables voice commands. This feature, known as the Wuling Indonesian Command (WIND), allows users to control the vehicle using their voice in indonesian language (Bahasa). WIND has the capability to perceive and capture sounds in the Indonesian language (Pranadita, 2020). Given that key individuals/officials in Indonesia utilize the Wuling Almaz vehicle, it is evident that sensitive and crucial data can be effortlessly documented. This has the capacity to be stolen.

ADAS can gather vehicle location data using the Global Positioning System (GPS) integrated into the car. Cameras, radar, and LiDAR can provide image information of the car's surroundings. The Wuling Almaz cars have a feature called Wuling Interconnected Smart Ecosystem (WISE), which allows access to digital information and data through the internet of vehicle (IOV) technology. The Wuling Almaz car is equipped with the Wuling Indonesian Command (WIND) system, allowing users to control the vehicle via voice commands. This system utilizes a microphone in the car cabin to capture sound. Based on the features and sensors employed on the Wuling Almaz, there is a possibility that ADAS might be utilized as a means of Chinese espionage.

According to Wuling sales consultants, the Wuling Almaz is equipped with a remote-control feature accessible through MyWulingPlus. This feature allows the vehicle owner to start the engine of the vehicle in Jakarta while they are in Bali for example, in order to warm up the engine. Additionally, the driver can also activate the air conditioner remotely to cool down the vehicle. Prior to boarding the vehicle, we can enter the Wuling Almaz car cabin by using MyWulingPlus, which can be accessed using a smartphone. Another function of this app is to track the vehicle's whereabouts. When fully utilized, the Wuling Almaz uses ADAS to remotely control the vehicle. However, this poses a risk of information leaks, including the vehicle's location and access to the radar, LiDAR, and camera sensors on the Wuling Almaz. According to He et al. (2020), the Wuling Almaz belongs to the category of Connected and Autonomous Vehicles (CAV), making it highly susceptible to cyber threats.

4.2. Vulnerability of espionage activities in the Wuling Interconnected Smart Ecosystem (WISE)

The Indonesia Cyber Security Forum (ICSF) specialists conducted a risk analysis evaluation on ADAS. ADAS technology can potentially facilitate espionage due to the presence of the Wuling Interconnected Smart System (WISE) feature, which creates prospects for information data breaches. An approach involves examining instances of information breaches that frequently transpire within governmental organizations. Hence, it can be inferred that China could potentially utilize ADAS technology as a means of conducting espionage.

If the network system and components are sourced from China, the utilization of ADAS can impact the occurrence of information leakage (Sheik et al., 2024). ADAS technology employs a multitude of components, rendering concealed components compromised in the ADAS system more readily camouflaged and challenging to identify. Hence, it may be inferred that the advancement of ADAS technology has an impact on the occurrence of Chinese espionage.

According to experts from the Indonesia Cyber Security Forum, the utilization of ADAS brings various vulnerability threats, particularly in the case of the Wuling Almaz, which incorporates an internet of vehicle function. The Wuling Almaz experiences frequent supply disruptions in its electrical devices due to the intricate transmission network comprising several delicate components that are very susceptible to compromise, making it exceedingly challenging to prevent such occurrences. It is important to carefully assess the implementation of advanced driver assistance systems or self-driving technology in relation to the necessary legislation and policies that govern electronic components. This is to ensure that national interests and security are not compromised. The utilization of ADAS technology possesses significant promise as a means for conducting espionage activities.

By examining the effect variables, it can be argued that the utilization of ADAS as a means of espionage has the capacity to emerge as a novel intelligence gathering technique through the usage of vehicle-based technology. ADAS enables the collection of visual information using 360-degree cameras on the vehicle. The Wuling Indonesian Command (WIND) system collects sound information. The Wuling Almaz, equipped with the Wuling Interconnected Smart Ecosystem feature (WISE), allows for information collection and leakage. This is possible through direct vehicle network connectivity or via smartphones with the Mywulingplus application. Consequently, the information security system of the Wuling Almaz is vulnerable. The WISE diagram is as in Figure 1.

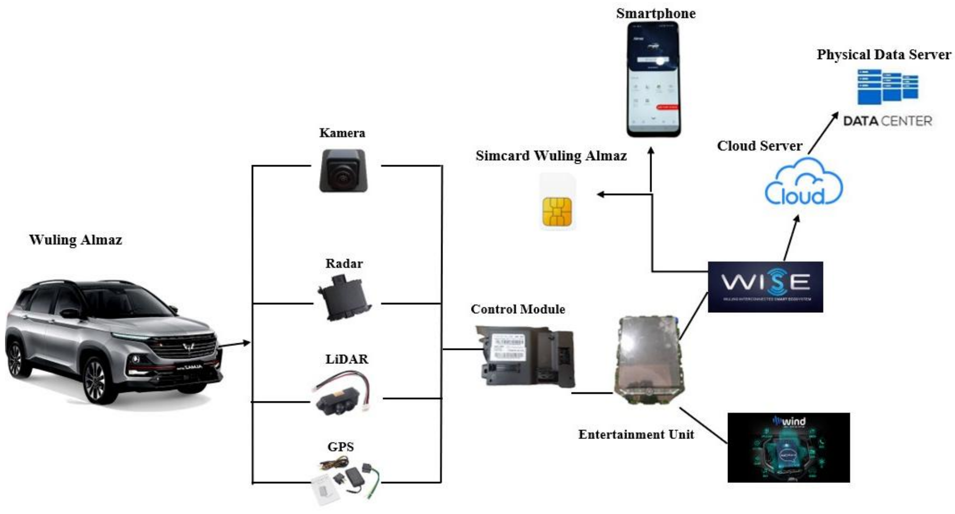

Figure 1. The Wuling Interconnected Smart Ecosystem (WISE) working system.

The Wuling Almaz is equipped with many sensors, including cameras, radar, LiDAR, and GPS, which are all connected to a control module. This control module plays a crucial role in managing the vehicle's electrical system. Control modules encompass several sorts and distinct purposes. For instance, the transmission module is responsible for regulating the gearbox, the engine control module is tasked with initiating and halting the engine, and the body control module oversees the vehicle's electrical system. The control module transfers electrical power to the entertainment unit located on the car dashboard.

Within the entertainment unit, there is a motherboard responsible for controlling the sensors, processing data, and displaying the features that are now in operation. The entertainment unit is equipped with the Wuling Interconnected Smart Ecosystem (WIND) and Wuling Indonesian Command (WIND) capabilities. The Wuling Almaz has the capability to utilize either the network provided by the sim card integrated into the vehicle or the network from the smartphones of registered drivers using the MyWulingplus application.

The WISE system on Wuling Almaz stores user or driver data on a Cloud server, which requires a real data center or a dedicated data center building. The Wuling Hongguan firm refrains from revealing the whereabouts of the data center, so significantly amplifying the susceptibility of the vehicle. The Wuling Almaz utilizes the Wuling Interconnected Smart Ecosystem (WISE) work system, which relies on an internet network provided by the sim card installed in Wuling Almaz vehicles and smartphones. However, there is a vulnerability in WISE as it utilizes a cloud-based virtual server system, with each virtual server including physical server data. Nevertheless, the Wuling data center is not located in Indonesia, and diligent researchers have conducted a thorough investigation to ascertain its whereabouts, only to come up empty-handed.

As a result of the ease with which users can command the Wuling Almaz car from a remote location, the WISE system is vulnerable to being hacked or used on purpose as a tool for espionage. The network on the Wuling Almaz continues to function as long as the car is in a location that has a strong connection, and the battery is fully charged. This presents a considerable risk because the network is active (Knüsel, 2020).

4.3. The possibility of wiretapping through the Wuling Indonesian Command (WIND)

The Voice Command feature in vehicles is a technological innovation that enables drivers to control numerous components in the vehicle by giving voice commands or directions (Bilius & Vatavu, 2020). The voice command capability on the Wuling Almaz is referred to as the Wuling Indonesian Command (WIND). The voice command feature integrated into the Wuling Almaz is designed to enhance safety and convenience by enabling the driver to remain attentive to the road without the need for manual adjustments or tapping buttons on the vehicle's control panel.

Several typical functionalities that can be accessed with Voice Command encompass: Navigation, the driver has the ability to utilize voice commands to input a desired location or obtain directions directly from the vehicle's navigation system. The Music and Media Playback feature enables the driver to manage the playback of music, radio, or other media sources without the need to physically interact with the vehicle's control panel. By utilizing voice command, drivers have the ability to instruct the system to initiate phone calls with certain contacts or respond to incoming calls without the need to physically interact with their mobile device. The driver has the capability to issue vocal commands in order to modify various car configurations, including seat adjustments, interior temperature, and other settings. Basic commands Certain voice command systems possess the capability to comprehend broad orders or inquiries, such as inquiring about the weather, specifying a preferred radio station, or doing a search for specific information.

The technology utilizes advanced speech recognition algorithms to accurately interpret differences in accent, intonation, and vocal characteristics. This enables the voice command system to accurately identify the driver's tone. The Wuling Almaz's voice command feature, which relies on a microphone sensor to capture sound, poses a vulnerability to voice eavesdropping. This is due to the continuous connection between the vehicle and the voice command system, allowing easy access to eavesdrop on important figures and officials. The term "government" refers to the system or group of individuals that have the authority to make and enforce laws and regulations within a particular country or region.

Due to the fact that the Wuling Almaz vehicle maintains a continuous connection to the internet network through the Internet of Vehicle feature, occasionally referred to as the Wuling Interconnected Smart Ecosystem (WISE) function, voice tapping is a possibility. Considering that customers are unable to block data transfers, the WISE function that is available on Wuling Almaz automobiles enables open connectivity, which in turn makes it possible for a variety of espionage actions to take place (Rivera et al., 2022).

4.4. Assessment of the Risk Level Posed by the Advanced Driving Assistance System on the Wuling Almaz to National Security

As per the analysis of a cyber security expert, the United States currently holds a dominant position in the control of application and programming software technology, while China has a stronghold on the hardware components of devices. This is primarily due to China's ability to sell technology components for computers at low prices while maintaining high specifications. It is worth noting that even American products often rely on hardware sourced from China, which poses potential risks as the hardware components may contain embedded chips. China possesses the most optimal components and offers the most competitive costs. However, Indonesia currently lacks the necessary technological capabilities to independently manufacture its own hardware.

To protect software and hardware from the risk of information leakage, encryption is employed. China has progressively assumed a prominent position in the manufacturing of hardware components in recent decades (Hou & Wang, 2020; Madeleine, 2023; Russell, 2007). China's expertise in manufacturing hardware components is primarily due to its robust manufacturing infrastructure. China possesses an extensive and exceptional manufacturing infrastructure. The Chinese government has made significant investments in constructing industrial facilities, including factories that manufacture hardware components such as microprocessors, memory chips, and other electronics. China offers cost-effective labor as its labor expenses are comparatively lower than those of many other wealthy nations. China has become an appealing destination for multinational corporations to relocate a significant portion of their manufacturing operations in order to lower production expenses.

Worldwide network of interconnected businesses involved in the production, distribution, and delivery of goods and services. China has effectively established a sophisticated and seamlessly connected worldwide supply chain. A multitude of international corporations engage in collaboration with manufacturers in China to fabricate their components and hardware. One notable example is Foxconn, a crucial manufacturing collaborator for numerous multinational technology corporations.

The effectiveness of an Advance Driver Assistance System (ADAS) relies on various elements, including the specific technology employed, the resources at hand, and the intended purpose. While it cannot be definitively shown that this technology is being used for espionage, there is a possibility that it could represent a threat to national security if misused. Hence, it is imperative to do meticulous risk assessment and meticulous strategic planning while utilizing this technology. Currently, there are no precise benchmarks available for evaluating the potential risks associated with the use of ADAS (Advanced Driver Assistance Systems). Nevertheless, under the most unfavorable circumstances, the utilization of ADAS in Wuling Almaz automobiles could potentially jeopardize the stability of national security.

4.5. ADAS at Wuling Almaz for Gathering Strategic Information: Mitigation Efforts

Derived from expert interviews, here are three measures to counteract espionage at Wuling Almaz.

4.5.1. Safety Regulations and Standards

To establish regulations for Advance Driver Assistance (ADAS) electronic components at Wuling Almaz, one approach is to develop backdoor scanning tools through BSSN or technology security and network information system vendors. These tools should be capable of efficiently scanning the numerous components in ADAS hardware. Wuling should enhance the security of the ADAS system as well. Additionally, the government is obligated to establish regulations for the utilization of any and all data collected from connected vehicles (Lee & Hess, 2020).

4.5.2. Data Encryption

Government agencies, particularly the State Intelligence Agency and the National Cyber Crypto Agency (BSSN), are required to conduct studies, research, and development of encryption that may be utilized on imported hardware components. This is due to the fact that these components are extremely susceptible to being infiltrated by backdoors. In its capacity as a national encryption organization, BSSN exerts a significant amount of influence over the safety of information systems and networks in both governmental offices and the general public. It is hoped that the encryption that was created or developed directly by BSSN will be able to overcome the presence of malware that is found in network information systems in Indonesia. Additionally, it is hoped that the encryption will be able to provide protection for privacy, data security, certainty of data integrity, data protection, and protection for systems that create user trust towards a system. During the process of data storage and transfer, it is important to implement a robust data encryption system in order to safeguard data information, particularly that which is gathered by ADAS (Lee & Hess, 2020). According to Olutola & Olumuyiwa (2023), AES (Advanced Encryption Standard) is a superior choice for data encryption compared to the Rivest Shamir Algorithm (RSA) due to its advantages in terms of encryption and decryption time, key length, and buffer length.

4.5.3. Software Updates

Implementing software updates supplied by developers has been found to be efficient in addressing emerging malware threats. Additionally, utilizing paid or premium antivirus software has demonstrated the ability to effectively combat new forms of malware on a daily basis. Similarly, Wuling Almaz vehicles can protect against cyber espionage malware by regular software upgrades. It is necessary for Wuling corporation to give software updates to address any malware that may originate from external sources affecting the Wuling Almaz vehicle. Wuling offers regular software upgrades for ADAS systems to address newly discovered security vulnerabilities and ensure that customers may easily and promptly install these updates. Implementing updates to software is a highly effective method for addressing malware (Kafi & Akter, 2023).

4.6. Intelligence Analysis Results

4.6.1. Judgment

The presence of Advanced Driver Assistance Systems (ADAS) in Wuling Almaz automobiles poses a significant risk that might potentially compromise national defense and security. Technological advancements in the automotive industry, specifically in the form of Advanced Driver Assistance Systems (ADAS), can give rise to various types of threats. These threats include the mapping of critical national assets and strategic industrial sectors that are accessed by vehicles equipped with ADAS features. Additionally, there is a risk of eavesdropping and unauthorized disclosure of vehicle owner's cyber information that is stored in the cloud server-based WISE feature, particularly in the case of Wuling vehicles. The Wuling Almaz is equipped with a variety of sensors, including a camera, radar, LiDAR, and GPS. It also has autonomous IoT connectivity through an implanted SIM card. However, this feature poses a danger of information leaking when data is uploaded using the WISE feature on the Wuling Almaz.

4.6.2. Forecasting

The advancement of ADAS technology in vehicles will lead to a rising number of cars equipped with ADAS characteristics, hence raising the potential risk of espionage through vehicles. This is supported by the anticipated advancement of the automotive sector in 2025, which will establish ADAS as a fundamental and obligatory feature in every automobile industry. This implementation aims to enhance driving convenience and reduce the likelihood of traffic accidents.

Without the Indonesian government taking proactive measures to develop encryption and design backdoor scanning tools for electronic components in vehicles that utilize ADAS or similar driving assistance systems, there will inevitably be disorder in attempts to protect crucial national assets and safeguard strategic information in the face of the cascading consequences resulting from the misuse of ADAS. This misuse can have significant implications in areas such as the economy, espionage, defense, and national security.

4.6.3. Early Warning

There is a growing danger of espionage that targets important national assets, strategic industries, and the illegal exposure of sensitive information as a result of the widespread adoption and exploitation of the Advanced Driver Assistance System (ADAS). This danger extends to official government employees and national authorities that rely on automobiles that are fitted with advanced driver assistance systems (ADAS) and other similar driving assistance systems.

It is possible that certain organizations might potentially exercise substantial influence over the economy, defense, and national security through the deployment of ADAS. This could be accomplished by collecting data from automobiles that are equipped with ADAS or other driver aid systems that are comparable. Due to the fact that a considerable number of people are unaware of the current security vulnerabilities in these vehicles, the implementation of ADAS in automobiles not only has advantages in terms of espionage but also has advantages in terms of protection.

4.6.4. Problem Solving

In compliance with Presidential Decree No. 8 of 2021, the Ministry of Defense is required to enhance the execution of the General National Defense Policy for 2020-2024. To facilitate this enhancement, BSSN, BIN, KOMINFO, the Ministry of Defense, and the Ministry of Industry must promptly engage in discussions to devise a strategic plan for the next five years. This plan should focus on fortifying security in the cyber security sector, particularly for electronic components. The purpose of the import is to proactively address any risks that may arise from the usage of driving assistance technology in Indonesia, both in domestically produced and imported automobiles. Additionally, it aims to educate the public and raise awareness about cyber information security.

5. Conclusion

By correlating the data from the sources in this research, ADAS could be used for espionage. The Indonesian government struggles to optimize data and information security and supervise electronic components entering from overseas, especially China, which is inversely proportionate to the impact and risks of modern technology. There are no clear laws to deal with cybercrime because cybercriminals in the form of groups or state actors cannot be enforced by law, and if there is a potential threat from the use and use of the ADAS in Wuling Almaz, it could be used as a media for espionage, which is another obstacle to regulating the use of driving assistance to increase driving safety. Thus, new regulations are needed to allow modern vehicles to use driving aid technologies to reduce traffic accidents. It can be concluded that ADAS could be used for espionage, which could affect national security, and that there is a high risk of vulnerability, especially for countries like Indonesia that have encryption weaknesses and lack cyber security knowledge. Internet-connected electronic devices are commonly involved. There is no significant support to optimize BSSN's role and function as a government agency tasked with minimizing the impact and risks of cyber information leakage activities related to the potential use of internet-connected electronic device components. Thus, ADAS technology must be monitored and regulated to avoid harming the environment and society and protect national stability and security.

References

Azevedo, P., & Santos, V. (2024). Comparative analysis of multiple YOLO-based target detectors and trackers for ADAS in edge devices. *Robotics and Autonomous Systems*, *171*(October 2023), 104558. https://doi.org/10.1016/j.robot.2023.104558

Bilius, L.-B., & Vatavu, R.-D. (2020). A multistudy investigation of drivers and passengers' gesture and voice input preferences for in-vehicle interactions. *Journal of Intelligent Transportation Systems*, *25*(2), 197–220.

Blanchard, A., & Taddeo, M. (2023). The ethics of artificial intelligence for intelligence analysis: a review of the key challenges with recommendations. *Digital Society*, *2*(1), 12.

Chiu, P. E., Lin, S. C. A., Li, Y. P., Huang, C. H., Shu, Y. M., & Chen, C. W. (2024). Experience in professional resilience for nurses caring for patients with COVID-19: A qualitative descriptive study. *Asian Nursing Research*, *18*(1), 28–35. https://doi.org/10.1016/j.anr.2024.01.003

DeGuzman, C. A., & Donmez, B. (2022). Drivers don't need to learn all ADAS limitations: A comparison of limitation-focused and responsibility-focused training approaches. *Accident Analysis and Prevention*, *178*(August), 106871. https://doi.org/10.1016/j.aap.2022.106871

He, Q., Meng, X., & Qu, R. (2020). Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles. *Journal of Advanced Transportation*, *1*, 6873273. https://doi.org/10.1155/2020/6873273

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). *Computers and Security*, *98*(2020), 102019. https://doi.org/10.1016/j.cose.2020.102019

Ji, B., Zhang, X., Mumtaz, S., Han, C., Li, C., Wen, H., & Wang, D. (2020). Survey on the internet of vehicles: Network architectures and applications. *IEEE Communications Standards Magazine*, *4*(1), 34–41.

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15–26.

Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis and Prevention*, *148*(May), 105837. https://doi.org/10.1016/j.aap.2020.105837

Knüsel, A. (2020). Swiss counterintelligence and chinese espionage during the cold war. *Journal of Cold War Studies*, *22*(3), 4–31.

Lee, D., & Hess, D. J. (2020). Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization. *Transportation Research Part A: Policy and Practice*, *136*(March), 85–98. https://doi.org/10.1016/j.tra.2020.03.026

Madeleine, R. (2023). *Chinese tracking device is "discovered inside UK government car", as senior politician slams Beijing as a "systematic" threat to Britain's security*. https://www.dailymail.co.uk/news/article-11607735/Chinese-tracking-device-discovered-inside-UK-government-car-senior-politician-slams-Beijing.html

McCall, S., Yucel, C., & Katos, V. (2021). Education in cyber physical systems security: The case of connected autonomous vehicles. *IEEE Global Engineering Education Conference, EDUCON*, 1379–1385. https://doi.org/10.1109/EDUCON46332.2021.9454086

Nandavar, S., Kaye, S. A., Senserrick, T., & Oviedo-Trespalacios, O. (2023). Exploring the factors influencing acquisition and learning experiences of cars fitted with advanced driver assistance systems (ADAS). *Transportation Research Part F: Traffic Psychology and Behaviour*, *94*(March), 341–352. https://doi.org/10.1016/j.trf.2023.02.006

Ogasawara, M. (2022). Legalizing illegal mass surveillance: A transnational perspective on Canada's legislative response to the expansion of security intelligence. *Canadian Journal of Law and Society/La Revue Canadienne Droit et Société*, *37*(2), 317–338.

Olutola, A., & Olumuyiwa, M. (2023). Comparative analysis of encryption algorithms. *European Journal of Technology*, *7*(1), 1–9. https://doi.org/10.47672/ejt.1312

Pesé, M. D., Pu, X., & Shin, K. G. (2020). Spy: Car steering reveals your trip route! *Proceedings on Privacy Enhancing Technologies*.

Phillips, P. J., & Pohl, G. (2024). Information, uncertainty & espionage. *The Review of Austrian Economics*, *37*(1), 35–54.

Pranadita, N. (2020). The use of artificial intelligence to reveal negative impact of a products legally as an understanded side. *2nd Social and Humaniora Research Symposium (SoRes 2019)*, *409*, 187–190. https://doi.org/10.2991/assehr.k.200225.038

Qin, Y., Tang, A., Jia, J., Wan, L., Zhao, H., & Long, Y. (2022). Research on radiated immunity test methods for adas functions considering vehicle in-the-loop. *World Electric Vehicle Journal*, *13*(11). https://doi.org/10.3390/wevj13110211

Reuters. (2021). *Tesla cars banned from China's military complexes on security concerns -sources.* https://www.reuters.com/article/idUSKBN2BB18R/

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An analysis of cyber espionage process. *Developments and Advances in Defense and Security: Proceedings of MICRADS 2021*, 3–14.

Russell, R. L. (2007). *Sharpening strategic intelligence: Why the CIA gets it wrong and what needs to be done to get it right.* Cambridge University Press.

Saheb, T. (2023). Ethically contentious aspects of artificial intelligence surveillance: a social science perspective. *AI and Ethics*, *3*(2), 369–379.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*, 1–29.

Seacrist, T., Maheshwari, J., Sarfare, S., Chingas, G., Thirkill, M., & Loeb, H. S. (2021). In-depth analysis of crash contributing factors and potential ADAS interventions among at-risk drivers using the SHRP 2 naturalistic driving study. *Traffic Injury Prevention*, *22*(sup1), S68–S73.

Sheik, A. T., Maple, C., Epiphaniou, G., & Dianati, M. (2024). Securing cloud-assisted connected and autonomous vehicles: An in-depth threat analysis and risk assessment. *Sensors*, *24*(1). https://doi.org/10.3390/s24010241

Soegirman, S. (2009). *Analisis intelijen sebuah kontemplasi*. CSICI.

Wallace, R., Melton, H. K., & Schlesinger, H. R. (2009). *Spycraft: the secret history of the CIA's spytechs, from communism to Al-Qaeda*. Penguin.

Whalen, J. (2024). *U.S. launches investigation of Chinese vehicles, citing security risks*. https://www.washingtonpost.com/technology/2024/02/29/us-investigation-chinese-vehicles/

Wood, J. M., Henry, E., Kaye, S. A., Black, A. A., Glaser, S., Anstey, K. J., & Rakotonirainy, A. (2024). Exploring perceptions of Advanced Driver Assistance Systems (ADAS) in older drivers with age-related declines. *Transportation Research Part F: Traffic Psychology and Behaviour*, *100*(October 2023), 419–430. https://doi.org/10.1016/j.trf.2023.12.006

Wuling. (2022). *Almaz RS EX, flagship SUV Wuling with special offers and various modern features*. https://wuling.id/en/blog/press-release/almaz-rs-ex-flagship-suv-wuling-with-special-offers-and-various-modern-features

Zou, J., Xie, J., Zhang, J., Zhao, H., & Lu, P. (2024). Coping trajectory of social isolation in individuals with maintenance haemodialysis: A descriptive qualitative study. *International Journal of Nursing Studies Advances*, *6*(November 2023), 100193. https://doi.org/10.1016/j.ijnsa.2024.100193