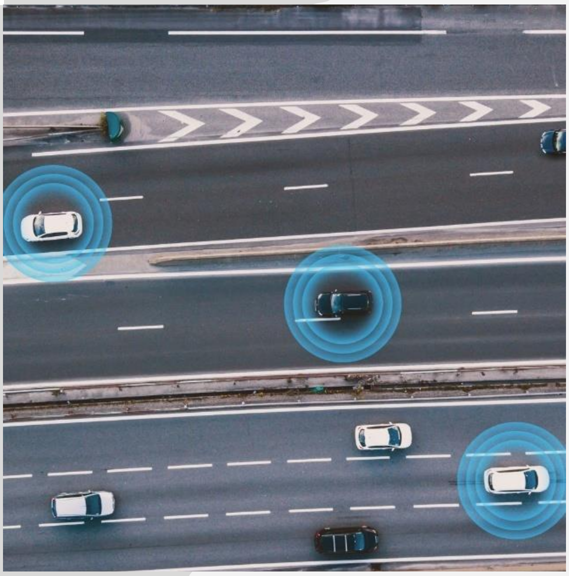
CKN China Kennisnetwerk

Evaluating Data Security in Chinese Drones and Smart Vehicles

A CKN Report



Rogier Creemers

John Lee

April 2025

About the authors

Rogier Creemers is a Lecturer in Modern Chinese Studies. With a background in Sinology and International Relations, and a PhD in Law, his research focuses on Chinese domestic digital technology policy, as well as China's growing importance in global digital affairs. He is the principal investigator of the NWO Vidi Project "The Smart State: Big Data, Artificial Intelligence and the Law in China". For the Leiden Asia Centre, he directs a project on China and global cybersecurity, funded by the Dutch Ministry of Foreign Affairs. He is also a co-founder of DigiChina, a joint initiative with Stanford University and New America.

John Lee is director of the consultancy East West Futures. He is also a researcher at the LeidenAsiaCentre, Co-lead on the EU China Semiconductor Observatory, and TOY Senior Fellow with Asia Society Switzerland and Fellow at the Asia Society Policy Institute's Center for China Analysis. John's research focuses on China and digital technology, in particular China's cyberspace governance regime, the semiconductor industry and future telecommunications networks. Previously he was a senior analyst at the Mercator Institute for China Studies and worked at the Australian Department of Foreign Affairs and Trade and the Department of Defence.

The authors would like to thank the researchers behind Project Lion Cage for their assistance.

This report was published under the framework agreement for the China Knowledge Network (CKN) funded by the Dutch Ministry of Foreign Affairs, for knowledge exchange with all Dutch ministries regarding policy challenges and opportunities related to China. The responsibility for the content and expressed opinions lies solely with the authors. The network is managed by the Dutch ministry of Foreign Affairs, the Netherlands Institute of International Relations 'Clingendael' and the LeidenAsiaCentre.

The Netherlands Institute of International Relations 'Clingendael' is a leading independent think tank and academy on international relations. The LeidenAsiaCentre is an independent research centre affiliated with Leiden University. It serves as a hub for applied academic knowledge on modern Asia.

Table of contents

1. Introduction and context

Digital technologies are profoundly transforming the way that consumers engage with products. On the one hand, they have drastically impacted the functioning of traditional goods. In cars, electronics have rapidly evolved from relatively simple applications in engine management and diagnostics to include infotainment and advanced driver aids such as adaptive cruise control, lane-keeping systems and parking assistance. A next generation of technologies, including vehicle-to-everything (V2X) communication and automated driving are gaining increasing adoption. On the other hand, they have enabled the emergence of new product categories. The market for consumer unmanned aerial vehicles (UAVs)[1] has rapidly expanded, as drones became cheaper and more advanced at the same time. The EU's 2022 European Drone Strategy 2.0 estimates that the drone market could grow to 30 billion EUR in scale and create 154.000 jobs by the end of this decade[2]. Their scope of application ranges from mundane individual hobbies to applications in mapping, surveying and pollution control. Pilot projects for drone-enabled logistics and deliveries are underway.

Key to the functioning of these digitized products is data and connectivity. Smart vehicles collect data related to the performance of hardware and software, as well as the individuals on board the routes they take and their surroundings. In some cases, that data is transferred out of the vehicle, for instance to manufacturers for the sake of later updates or training autonomous driving algorithms. Drones are primarily used to gather data one way or another through cameras and on-board sensors, and require continuous data connectivity with their operators for operations and safety purposes. This core function of data and connectivity is only likely to intensify, for instance as vehicles will communicate ever more with other vehicles and smart infrastructure, or as businesses create new data-enabled products and services around these products.

Yet this new centrality of data and connectivity raises questions concerning data and cyber security. Data can be valuable to malicious actors, whether criminals or spies, while the devices generating them may be vulnerable to sabotage or even hijacking. Particular unease is growing for geopolitical reasons, and more specifically the growing presence of Chinese manufacturers in the car industry, as well as their dominance of drone production. Echoing earlier distrust of Huawei and ZTE in the telecommunications sector, Western governments are ratcheting up scrutiny of Chinese data-enabled products on their markets, with Washington in the lead. In March, the US government started an investigation into the potential national security risks posed by Chinese vehicles[3], leading to the institution of nationwide restrictions on the sale of Chinese connected passenger cars, as well as smart vehicle software and hardware[4]. Since 2017, various US government bodies have alleged drones made by the Chinese company and market leader

[1] Also referred to as "drones" in this report.

[2] https://transport.ec.europa.eu/news-events/news/drone-strategy-creating-large-scale-european-drone-market-2022-11-29_en

[3] https://www.reuters.com/business/autos-transportation/us-says-investigate-national-security-data-risks-chinese-vehicles-2024-02-29/

[4] https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary?mc_cid=dc1afb15b7&mc_eid=ad7c94e0d8

contain espionage and surveillance backdoors, culminating in a 2023 prohibition for all federal agencies to use Chinese drones. At the time of writing, the Countering CCP Drones Act has passed the House of Representatives, awaiting a vote in the Senate. This would, amongst others, ban new DJI UAVs from US communications networks[5]. Sometimes, these concerns go far: in the Netherlands, a The Hague city councillor called for a "thorough investigation" about the espionage risks stemming from using BYD vehicles in a municipal service to transport disabled and elderly individuals[6].

In most of the policy processes and public debate surrounding these issues, it is often assumed that Chinese companies will find it difficult to resist pressure from the Chinese government, amongst others because of provisions in intelligence legislation stipulating that Chinese firms must collaborate with intelligence services when asked to do so[7]. In addition to intelligence legislation, the Chinese government has also passed several pieces of general legislation, as well as sector-specific regulation, to manage the collection, storage, processing and use of data, including potential government access to data. It is certainly the case that Chinese intelligence services are building up their capabilities to obtain large-scale data about priority targets, of which the Netherlands is likely one. They also face far less constraints through oversight processes or judicial institutions. But the risk calculus of European governments cannot be black and white. The nature and impact of risk depends on which technologies, users and applications are involved. Risks can only be excluded by eliminating Chinese products, components and technologies from consumer markets, but that would carry potentially significant costs. Closing European markets to Chinese products might invite retaliation, deny high-quality, innovative products to EU consumers and users, affect partnerships between European and Chinese companies, or hinder Chinese investments into Europe-based business activities.

To assist this effort, this report will review whether China's legal frameworks for data governance create or increase risks for Dutch and European companies, individuals, infrastructure and national security, whether the Chinese government can leverage this legislation to affect the confidentiality, integrity and availability of personal and corporate data of Dutch and European citizens, companies, organizations and government bodies. Its first section will focus on the legal and policy-strategic aspects of Chinese data regulation, exploring the extent to which Chinese law enables access to sensitive information. The second section specifically addresses the case studies of smart vehicles and drones, reviewing the technical aspects of related data flows and discussing the state of technical standardization. The third section summarizes the report's findings, and offers policy recommendations. For the purposes of this report, the focus concerning smart connected vehicles is on battery electric consumer vehicles (instead of, for instance, buses and other public transport vehicles), and concerning UAVs is on commercial (not military use) drones.

[5] https://dronelife.com/2024/06/15/ndaa-passed-the-house-what-that-means-for-the-countering-ccp-drones-act-and-what-comes-next/

[6] https://vvddenhaag.nl/vrees-voor-spionage-china/

[7] See, for instance, https://blog.merics.org/en/comment/data-quagmire-german-carmakers-china; https://www.lawfaremedia.org/article/legal-aspects-banning-chinese-drone-technology

2. Legal, policy and strategic aspects of data legislation in China

This section will provide an overview of China's legal framework for data governance, focusing particularly on data collection, processing and storage, as well as the policy context in which they have emerged. It will do so in four sections. First, it will provide an introduction to the overall landscape within which this framework has been constructed. Second, it will address the level of data-specific legislation, including the Personal Information Protection Law and the Data Security Law. Third, it will review sector-specific regulation governing the specific products analysed in the case study: smart vehicles and consumer drones. Fourth, it discusses whether and how the National Intelligence Law might be applied to coerce Chinese manufacturers to provide data collected abroad to intelligence and security services.

2.1 The data policy environment

Over the past decade, the Chinese government has demonstrated a growing awareness of the importance of data, both as an economic resource and as a security concern. In its data policy, it has therefore sought to balance a developmental approach, focused on enhancing the value of data for China's economic growth as well as state governance capacity, with imposing stricter security requirements for both personal and non-personal data[8].

The first dedicated policy for data came in 2015, when the Action Plan on Big Data stated it had become a "basic strategic resource"[9]. On the basis of this document, refined in a subsequent five-year plan[10], government has built up a system of data centres and trading venues, industrial pilots, educational and research reforms, and supporting regulations. A particularly dominant objective is the use of data to modernise and improve existing industrial sectors. At the same time, however, Chinese authorities were in the process of drafting the Cybersecurity Law, which contained the first basic data protection provisions at the legislative level. This, and other digital security-related developments, were triggered by a series of data security concerns, most notably the Snowden revelations[11].

In the near-decade since then, Chinese data policy has pursued an elusive balance between enhancing the protection of data security and unleashing the economic value of data as part of industrial policy. The data protection legislation discussed below, for instance, also gave rise to a highly onerous framework for data export with a highly negative impact on cross-border data flows, affecting both international and domestic businesses. On the other hand, the State Council designated data to be a critical factor of production, on par with economic inputs such

[8] For a comprehensive account of this evolution, see https://academic.oup.com/cybersecurity/article-abstract/8/1/tyac011/6674794

[9] https://chinacopyrightandmedia.wordpress.com/2015/08/31/outline-of-operations-to-stimulate-the-development-of-big-data/

[10] https://cset.georgetown.edu/publication/14th-five-year-plan-for-the-development-of-the-big-data-industry/

[11] See: Creemers, Rogier. "Cybersecurity Law and regulation in China: Securing the smart state." *China Law and Society Review* 6.2 (2023): 111-145.

as land, labour and capital, in 2020[12]. 2023 saw the establishment of a new government body, the National Data Administration, with a mandate to create legal and policy frameworks for the development of data markets and other commercial applications of data[13]. The 14th Five-Year Plan for National Informatization highlights the use of data both in fostering new business models and in transforming traditional industries as China searches for new sources of economic growth[14].

2.2 Legislation: the Personal Information Protection Law and the Data Security Law

China's data protection system consists of two main components, revolving around respectively the Personal Information Protection Law and the Data Security Law, which both took effect in 2021. Further legislative measures are underway: a new administrative body – the National Data Administration – was established in 2023 to set rules for a data-enabled economy. However, none of these efforts has evolved to formal legislative drafts thus far.

2.2.1 The Personal Information Protection Law (PIPL)

The PIPL's[15] taking effect in 2021 concluded a decade of efforts to construct a legal framework for the protection of personal information in China. To a significant degree, it resembles – or is even based on – Europe's General Data Protection Regulation. As such, it establishes basic principles such as data minimization, necessity and consent. However, where the GDPR serves to realise the fundamental right of privacy guaranteed under EU law, China's PIPL is more purpose-driven in nature. Its primary objective is to protect individuals against abuse of their data by private sector actors: many of the Law's provisions seem to be targeted against large-scale online service providers. In addition, throughout the drafting process, legislators included provisions explicitly limiting personal information-based business models, such as prohibiting the refusal of services in case a data subject refuses to provide their personal information. Second, it also serves to strike a balance between the need of public authorities to access data easily in order to fulfil their statutory mandates and the frequent phenomenon of officials unlawfully selling government data on private markets. Lastly, the PIPL provides basic provisions for the export of personal data.

Most importantly for the purpose of this report, the PIPL sets its own jurisdictional boundaries as processing the personal information of individuals within Chinese territory by domestic or foreign actors – in the latter case only where the purpose of such processing is to provide products or services to such individuals, or analyse their activities. Given the fact that the EVs and drones studied in this report are not intended to do so (as they are sold to European consumers), they are

[12] https://digichina.stanford.edu/work/china-wants-to-put-data-to-work-as-an-economic-resource-but-how/

[13] https://policyreview.info/articles/news/chinas-national-data-bureau-and-global-data-governance

[14] https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/

[15] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

not covered by the provisions of the PIPL. *Prima facie,* therefore, the PIPL cannot be used as a legal basis to compel Chinese firms to provide information to Chinese government bodies on individuals outside of Chinese territory. As a result, the risks to Dutch personal information stemming from the potential extraterritorial application of the PIPL are very low.

2.2.2 The Data Security Law (DSL)

The Data Security Law[16] is, in many ways, a unique piece of legislation, with no immediate comparable parallel elsewhere in the world. Its purpose is to protect national security and the public interests against harm arising from the abuse of data - whether personal information or otherwise. Its core tenet is that data should be subdivided into three categories: ordinary data, important data and national core data, and that these should be subject to increasing demands concerning data safeguarding, security auditing and reporting, export restrictions, etc. However, as a very experimental legal tool, implementation and enforcement have been difficult. This problem starts with its general language: it contains many aspirational statements and mandates for government bodies to establish specific systems for data protection, but few immediately actionable provisions. Three years after its publication, there still is little clarity about how several of these terms are defined in practice, and therefore how businesses and other organizations should comply with them. This is largely due to the sheer difficulty of identifying every possible category of data and assigning a clear risk profile to them, but also due to competing interests surrounding these designations.

In terms of jurisdiction, the DSL is ambiguous on the question whether it applies outside Chinese territory, merely stating that if data handling activities abroad harm “the national security, public interests, or lawful rights and interests of PRC citizens or organizations”, legal liability will be prosecuted “according to the law”, without specifying which law that is. In any case, the DSL does contain a provision that enables law enforcement and national security bodies to require access to data, but stipulates that this requires “strict approval procedures according to relevant State provisions”[17], such as obtaining appropriate warrants. The law is silent on whether this provision can be applied to request access to data stored abroad, or whether other government bodies can demand access to data. Therefore, particularly given the fact that many aspects of the DSL remain underdeveloped, the current risks to Dutch data stemming from the DSL are low. This may, however, change over time as supporting regulatory frameworks mature, and therefore requires monitoring.

2.3 Sector-specific regulation

In parallel with the drafting of general data-related legislation, responsible authorities have also issued rules specific to industrial sectors and product categories. This section details provisions concerning data security present in such rules concerning smart vehicles and drones.

[16] https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

[17] DSL Article 35.

2.3.1 Automotive data

The Chinese Ministry of Industry and Information Technology (MIIT) has identified data security risks in smart vehicles as a policy priority for quite some time, issuing a first set of dedicated trial regulations in 2021[18]. These regulations apply to the entire lifecycle of a car, including design, production, sales, use, operation and maintenance, and cover data collection, storage, use, processing, transmission, provision to others and disclosure. They affect not only manufacturers, but also parts and software suppliers, dealers, maintenance providers and travel service companies. Building on the general definitions of personal information and important data in the PIPL and DSL, they further specify that: (1) ordinary personal information relates to identified or identifiable car owners, drivers, passengers, and people outside the car; (2) sensitive personal information includes vehicle tracking, audiovisual and biometric data; and (3) important information includes geodata as well as flows of vehicles and individuals in sensitive military and government facilities, important economic transportation and logistical data, operations data of EV charging facilities, extravehicular audiovisual data containing individuals' faces and licence plates, and large amounts of personal information. In addition to the obligation that any data processing is only connected with vehicle design, production, sales, use, operation and maintenance, the regulations establish four basic principles: (1) data must be processed inside the vehicle and transferred outside only if necessary; (2) the default setting must be to not collect data, which the driver must switch off before every drive; (3) collected data by cameras and sensors must be appropriate in scope and accuracy to their purpose; and (4) data must be anonymized wherever possible. Automotive data handlers must regularly conduct risk assessments and communicate them to regulatory authorities, and automotive data must be stored within China. Strict review requirements apply to automotive data export.

Separate provisions require automotive SIMs to be registered to individuals' ID documents[19]. Zhejiang provincial regulations even stricter: amongst others requiring a warning light when sensitive PI is collected[20]. EV manufacturer Xiaomi and cybersecurity standardization body TC260 are collaborating on a switch to shut down all extravehicular data collection[21]. Further draft standards by the Ministry of Natural Resources impose strict limitations on geospatial data, which may not be directly transmitted out of the vehicle or exported abroad. The collection of gravity data is restricted, and magnetic data is prohibited outright. Vehicles may not store coordinates of sensitive facilities, such as military bases and government compounds, and manufacturers will have to submit to compliance inspections[22]. Authorities have also paid particular attention to the security of surveying and mapping data. Such geographic information has long been seen as especially sensitive for national security reasons, but smart vehicles and smart infrastructure require extremely precise navigation information. Consequently, a range of regulations and standards, as well as higher protections under the Data Security Law (mapping

[18] https://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm

[19] https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_9b221a0452c043aaa1987307ad614be9.html

[20] https://mp.weixin.qq.com/s/2Cn7krdLC9oC0wcYTugBEA

[21] https://www.tc260.org.cn/front/postDetail.html?id=20240624102728&mc_cid=c23c388230&mc_eid=ad7c94e0d8

[22] https://www.huaxiataike.com/news/57579.html

data is one of the few categories explicitly designated as “important” under the DSL) , apply to geographic information[23].

Apart from these regulations, public security authorities were rumoured to have issued an order prohibiting foreign-branded smart vehicles from entering sensitive spaces[24]. This mostly ended up targeting Tesla, the most prominent US smart car brand on the Chinese market. Teslas have been banned from Beidaihe during the leadership’s annual summer retreat[25], the 2023 Chengdu World University Games[26] and even the car park of a small regional airport in Hunan province[27]. The specific reasons for these bans were rarely clear, but speak to the concern that Chinese officials too have about foreign smart vehicles as possible risks to data security. At least in the Beidaihe and Chengdu cases, Xi Jinping’s presence may have been an additional factor. It was only in 2024 that an official announcement came that Tesla had passed all data security compliance requirements[28]. Even so, it is still prohibited from exporting data, amongst others for the purpose of training its self-driving AI.

These regulations are only applicable within Chinese territory, and so do not legally affect Chinese-branded vehicles sold in European markets. They will, however, have a significant impact on how in-car data collection hardware and software are designed in the absence of EU regulation that would impose different compliance requirements (and bearing in mind global vehicle cybersecurity homologation standards discussed in the case studies below). In short, Chinese vehicles are developed in an environment where it is expected that data collection is minimised, detailed provisions apply to the handling of specific data and sensitive locations, and out-of-vehicle data transfer only takes place under very specific conditions.

2.3.2 Drone data

Although the drone industry lacks the scale of the automotive sector, it is growing rapidly. It currently is dominated by one player, the Chinese company DJI, which occupies over 70% of the market for consumer drones. From the Chinese policy perspective, they are particularly important as they enable the modernization of multiple economic sectors, as well as public services. For instance, the recent 14th Five-Year Plan for National Informatization envisions their use in the construction of sensing networks to be used for environmental monitoring,

[23] https://www.castc.net/news/9803.cshtml; https://auto.china.com.cn/view/20220830/719475.shtml; https://www.lexology.com/library/detail.aspx?g=5a8d4941-802b-4a2a-8e06-a6e8a1b2c8f7
[24] https://x.com/whyyoutouzhele/status/1699708953481854977
[25] https://www.reuters.com/business/autos-transportation/chinas-beidaihe-district-bar-tesla-cars-driving-july-local-police-2022-06-20/
[26] https://www.bloomberg.com/news/articles/2023-07-26/tesla-cars-barred-from-world-university-games-ahead-of-xi-visit
[27] https://www.sixthtone.com/news/1013528
[28] https://www.thepaper.cn/newsDetail_forward_27201728?commTag=true&mc_cid=88fdb4edfb&mc_eid=ad7c94e0d8

infrastructure building, urban management and agriculture[29]. Chinese companies are also experimenting with drones for smart logistics and package delivery[30].

In contrast to the automotive industry, there are no specific regulations on data collected by drones, although these might come in the future. Provisional general regulations on unmanned aerial vehicles were only finalized in May 2023, and came into effect on 1 January 2024 (UAV Management Regulations).[31] These are jointly issued by China's top civil and military institutions, the State Council and Central Military Commission. They stipulate that drones must carry a unique production identification code (UPIC) and must operate on the basis of real-identity verification of users. UPICs are governed by Chinese national standard GB/T 41300-2022, which specifies inter alia identification methods (bar code, QR code, electronic tag, radio broadcast).[32] They also expressly (Article 34(vii)) prohibit use of UAVs to 'illegally transfer data across the national border'. With the exception of micro-level drones (effectively toys), drone operators must obtain a certificate of operational compliance from civil aviation authorities. Illustrating the sensitivity of surveying and mapping, these activities require additional specific certificates. When they use their drones, operators must submit a flight plan 24 hours in advance, and avoid restricted flight areas. Public security authorities are empowered to manage and dispose of drones in situations of illegal flying or 'unclear situations'.

According to one official explanation of the UAV Management Regulations, they require operators to "report identification information to the UAV Integrated Comprehensive Supervision and Service Platform (UICSSP) during the flight process, and [...] automatically send identification information [...] realising traceability and full coverage of the UAV flight process"[33] The UICSSP is a cloud-based integrated system for drone management in China that is still under development, and will integrate the extant Civil UAV Integrated Management Platform ("Unified Operations Management System", UOMS) administered by China's Civil Aviation Administration (CAAC).[34] The intention is for the UOMS and ultimately the UICSSP, which will contain all UAV operational and flight data in China, to be integrated with the nation's general air traffic management system.[35]

MIIT has also issued regulations on the production of civil UAVs, which took effect from 1 January 2024 (UAV Production Regulations)[36]. These contain a few data security-related provisions: drone makers may not install malware, and must report cybersecurity vulnerabilities they discover. In addition, they must ensure their products are capable of "data traceability and data emergency

[29] https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/

[30] https://www.sixthtone.com/news/1015714

[31] https://www.gov.cn/zhengce/content/202306/content_6888799.htm

[32] https://std.samr.gov.cn/gb/search/gbDetailed?id=DAB8B4004620896BE05397BE0A0A0B32

[33] https://www.gov.cn/zhengce/202306/content_6888947.htm

[34] https://uom.caac.gov.cn/

[35]https://www.ecac-ceac.org/activities/unmanned-aircraft-systems/uas-bulletin/22-uas-bulletin/424-uas-bulletin-1-china

[36] https://jxt.zj.gov.cn/art/2024/3/29/art_1229560971_2516598.html

response in case of data security incidents", although little detail is available on how to specifically implement this requirement. The UAV Production Regulations specify that, again with the exception of "toy" drones, all civil UAVs manufactured in China must be assigned a UPIC that contains a name code, product code and serial number. The name and product codes must be reviewed and approved by MIIT before the items are put on the market, or prior to the first flight in the case of units that are used for test flights, assembly or subassembly. These UPICs will be part of a civil UAV production information system to be established by MIIT, to facilitate information sharing with local governments and with the UAV Integrated Supervision Service Platform.

Chinese authorities have been increasingly aware of the national security relevance of drones designed for civilian purposes. In June 2024, the MSS issued a post on its public WeChat account in which it detailed its handling of three cases where drones were flown close to classified military sites and sensitive areas, and resulting photographs were shared on public forums. This led, amongst others, to prison sentences for the operators involved on charges of illegally obtaining state secrets[37].

Another driver for drone regulations was the Russian invasion of Ukraine, where both sides have used Chinese-made drones for reconnaissance and attack purposes. In August 2023, the Ministry of Commerce announced export controls on drones and ancillary equipment, such as engines, lasers, communication equipment and anti-drone systems[38]. The export of civilian drones for military purposes was prohibited. In July 2024, the Ministry further strengthened export control standards for drones, particularly those equipped with high-precision measurement equipment[39].

These developments suggest that in China, like in Europe, regulators are becoming increasingly concerned with what happens when drones obtain data they shouldn't, particularly in case that data ends up in the hands of strategic adversaries. It is therefore likely that the next few years will see further regulation, imposition of technical standards and operator security requirements in the drone sector. Like in the automotive sector, this will incentivize drone manufacturers to heavily invest in product security, and to ensure the default mode of their products minimises data flows. To summarize, sector-specific regulations for both smart cars and UAVs suggest that Chinese authorities prioritize the security of these products over their hackability, at least at home. As the case studies below will discuss, these rules are also in line with international product standards. This suggests risks to Dutch data emerging from sector-specific regulations are not only low, but their compliant implementation will strongly reduce those risks.

[37] https://mil.news.sina.com.cn/2024-06-20/doc-inazisxp3392193.shtml

[38] https://www.reuters.com/world/china-curbs-exports-drone-related-equipment-amid-us-tech-tensions-2023-07-31/

[39] https://www.scmp.com/news/china/military/article/3272636/china-imposes-export-controls-drone-parts-military-and-civilian-use

2.4 Cybersecurity legislation and vulnerability disclosure

The 2016 Cybersecurity Law (CSL) was the first piece of dedicated legislation covering data security concerns, and in its data-specific provisions, has been nearly completely superseded by the PIPL and the DSL. For this reason, the CSL does not present additional potential risks above and beyond those discussed above with regard to direct Chinese government data held by smart car and UAV manufacturers, or their suppliers, including in the event of a data breach. However, the CSL ecosystem does contain another point worth mentioning: the obligation of companies to disclose cybersecurity vulnerabilities in their products to government bodies.

In 2021, the Ministry of Industry and Information Technology (MIIT), the Cyberspace Administration of China and the Ministry of Public Security jointly released regulations on managing digital security vulnerabilities[40]. These regulations require that when producers of digital products, software or hardware, discover a hackable vulnerability in their products, they must submit it to the MIIT's National Vulnerability Database within two days. According to an Atlantic Council report, this information is shared with the Chinese National Computer Network Emergency Response Technical Team/Coordination Centre (CNCERT/CC), which then supplies relevant information to, amongst others, the Ministry of State Security, China's spy agency, as well as to institutions associated with Chinese hacking campaigns in the past[41].

Patching discovered security vulnerabilities usually takes longer than two days, meaning these regulations create a de facto source of exploitable information for these Chinese government bodies. To be sure, this law does not uniquely apply to Chinese smart car and UAV manufacturers, but to all companies active in China, including European businesses. In several cases, European companies have complied with these legal requirements, although specific details remain unreported. Moreover, if patching a vulnerability takes time, so does writing the malware to exploit it, particularly if the information submitted by vendors is relatively low in detail. Nevertheless, this requirement would assist State-sponsored hackers in focusing their efforts on particular products of interest. Given the lack of publicly available information about the actual implementation of this framework, it is difficult to assess the degree to which these regulations would increase the risk of Dutch data being obtained through Chinese hackers exploiting vulnerabilities reported to them by smart car and UAV companies, and how that would differ from their non-Chinese competitors who must also comply with these regulations.

2.5 Intelligence legislation

In the security debate surrounding smart connected devices, such as smart vehicles and drones, mention is often made of the infamous Article 7 in China's National Intelligence Law, which compels "all organisations and citizens" to "support, assist and cooperate with national intelligence efforts". The oft-heard argument is that, in China's autocratic system, companies have no way of resisting demands from intelligence services to install backdoors, pass along

[40] https://www.chinalawtranslate.com/en/product-security-vulnerabilites/

[41] https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/

data, or otherwise assist surveillance and information gathering. Things are, however, not that simple. In the past, central authorities have often faced difficulties in getting businesses to hand over data[42], partially because that data constitutes a valuable corporate asset, partially because data protection practices within Chinese state bodies are lacklustre. In 2022, a database with details on over a billion Chinese citizens, including criminal records, ended up for sale on the Dark Web after it had effectively been left available and unsecured [43]. In a related area, cryptography, a similar tension is present. The revision of the Cryptography Law in 2019 went quite some way to liberalise market access for foreign encryption providers[44]. It also does not explicitly mention decryption, or any requirement that encryption keys and passwords are handed over to Chinese entities. Instead, it has moved towards requiring the encryption of data that may make government access and monitoring more difficult[45].

In addition, even within the law, several articles do provide a counterweight to these provisions. First, the Law does not contain any clear sanction or enforcement mechanism against individuals or companies that would refuse or otherwise fail to collaborate with intelligence services, only for actively obstructing their activities. Second, the law explicitly states that any such collaboration must proceed “according to law”. This suggests intelligence services cannot compel individuals or companies to break other laws (for instance, the PIPL and DSL) or subordinate regulations for the sake of collaboration with intelligence services. In addition, the next article in the NIL states that the “lawful rights and interests” of individuals asked to cooperate with intelligence services must be protected, and establishes channels for them to report improper conduct by these services.

To be sure, this form of recourse remains relatively weak, and there are no courts or other means of independent oversight that can provide a definitive constraint against Chinese security services’ attempts to coerce business into cooperation. Consequently, the actual probability that businesses such as BYD or DJI may be compelled by espionage agencies or security services to engage in such activities cannot be simply deduced from a black-letter reading of the law. It is also a political-economic question, depending on the panoply of interests and objectives within the Party-State constellation, where constraints on actions of intelligence services are determined to a significant degree by how the possible gains from such actions might offset costs and harms that would result elsewhere in the system.

This can only be done on a case-by-case basis. There are clear economic concerns: EV builders are central to maintaining a steady pace of economic growth in an economy facing increasing headwinds. Many EV builders are State-owned, which automatically gives them a voice in the system. Several private carmakers wield considerable political clout as well. BYD, for instance, is the largest non-State employer in China, with over 700.000 jobs. At a time of growing youth unemployment, Chinese central decision makers will likely try to avoid actions that would severely harm the global prospects of these national champions. Simply put, any meaningful

[42] https://www.ft.com/content/75409a44-6cfb-43e9-be31-776eb814a919

[43] https://www.nytimes.com/2022/07/07/business/china-police-database-hack.html

[44] https://www.chinalawtranslate.com/en/cryptography-law/

[45] https://carnegieendowment.org/posts/2021/03/the-encryption-debate-in-china-2021-update?lang=en

indication that Chinese smart vehicles are used systematically for surveillance and espionage would nearly immediately result in their exclusion from the lucrative global Northern market. Chinese intelligence chiefs will likely proceed on the basis that Chinese vehicles will be examined under a microscope in these markets, and that therefore any mass operation through them will be swiftly revealed. Furthermore, the mandated installation of backdoors and other vulnerabilities into these vehicles could also be exploited by foreign malicious actors, increasing risks on the Chinese side. Underlining the importance of case-by-case analysis, the drone industry, in contrast, does not carry the scale or political clout of the EV sector. Nevertheless, to build trust, market leader DJI Market leader has made explicit commitments to user privacy, as well as safety and security, as discussed below. The recommendations sector will further discuss options to mitigate risk for these two sectors.

3. Case Studies

3.1 Chinese made and designed intelligent connected vehicles (ICVs)

3.1.1 Chinese carmakers' presence in Western European markets

The presence of Chinese-branded vehicles in Europe is small but growing, particularly in Western Europe. According to one August 2024 study covering Western Europe - the 14 states that were EU members prior to the 2004 enlargement, plus Norway, Switzerland, Iceland and the UK, together accounting for over 95% of the total BEV volume in the enlarged European region - Chinese brands ('original equipment manufacturers', OEMs) accounted for 11% of new BEV registrations in Q2 2024. Three of the top five OEMs (by units) importing BEVs from China in Q2 2024 were Western brands (Tesla, Volvo, BMW/Mini), the other two being the Chinese brands MG (previously a UK brand, now owned by SAIC) and BYD. 95,533 new Chinese-brand BEVs were registered in H1 2024, SAIC brands accounting for over 45% of this total.[46]

Across all fuel types, registrations of Chinese brand passenger cars accounted for just 3.1% of Western Europe's total new car market over H1 2024 (although this rises to over 6% if including Volvo cars, Volvo being 79% owned by China's Geely). Around 400,000 Chinese-brand passenger cars are likely to enter Western Europe over 2024, a forecast that rises to just under 700,000 if including Western brands importing units manufactured in China. Assuming that the EU's tariffs targeting BEVs made in China are fully implemented for five years, Chinese OEMs' share of Western Europe's BEV new passenger car market is projected to peak in 2027 with just under 12% share of a 4.24 million unit market.

[46] Schmidt Automotive Research, Q2 2024 Nº1, Chinese OEM West European Market Intelligence Status Report -. Focus: BEVs (hereafter 'SAR Aug 2024') https://www.schmidtmatthias.de/electriccarreports/Quarterly-Chinese-Passenger-Car-Manufacturer-Performance-Study-focussing-on-BEV-models-Western-Europe-with-forecast-to-2030-p691949485

However these estimates do not include plug-in hybrid vehicles (PHEVs), which are not impacted by the new EU tariffs. Chinese market leader BYD through H1 2024 was offering only purely electric models in Europe, but is expected to introduce PHEV models in H2. BYD is also the Chinese OEM with most production capacity inside the EU Customs Union coming into operation, with car factories in Hungary and Turkey.

Furthermore, BYD is arguably the technological leader among the Chinese OEMs and the one best placed to exploit the cost advantages (notably falling prices for lithium-based batteries and silicon carbide-based power management semiconductors) that favour Chinese EV makers, due to BYD's high degree of vertical integration in its supply chain. For these reasons, it provides the first of two case studies below for data and cybersecurity considerations around Chinese OEMs' connected vehicles.

Other Chinese OEMs are also starting to make cars in Europe and import cars that they manufacture in third jurisdictions, notably the US and South Korea (which avoid the new EU tariffs). Some are reportedly seeking agreements with European contract manufacturers (Austria's Magna and Finland's Valmet) to assemble their models within Europe.[47] If the EU postpones automotive emissions targets currently scheduled for 2025, Chinese EV OEMs could further increase their share of the EU's BEV market in 2025 by one estimate up to 27%.[48]

3.1.2 Data security issues for intelligent connected vehicles (ICVs) and EU regulation

A recent submission by the European Automotive Manufacturers' Association to the US government describes the security environment for ICVs and the OEM's role:

> The vehicle manufacturer is responsible for securing any interface through which a vehicle communicates with the outside world. These interfaces are defined by the vehicle manufacturer [and allow for] controlled wireless communication of the vehicle's data to an off-board facility managed and secured by the manufacturer or a trusted partner, thereby providing end-to-end security from the vehicle [data] bus system to the hosting facility. Access by third parties to the data... is provided from the manufacturer's facility through a secure access point, managed by the manufacturer.[49]

Security issues around digitalisation of cars extend beyond unauthorised data access to critical safety functions, often illustrated by a 2015 demonstration of hackers remotely hijacking control of brakes and steering.[50] These potential threats are amplified by progress towards 'software-defined vehicles', meaning that a car's features and functions are primarily enabled and controlled through software. The push for higher levels of automated driving capability requires the introduction of artificial intelligence (AI)-enabled functions and more centralised computing architectures (as described in the BYD case study below). These industry-wide trends drive

[47] SAR Aug 2024.

[48] https://www.transportenvironment.org/articles/tariffs-wont-save-european-ev-manufacturing-if-eu-drops-co2-targets-analysis

[49] https://www.regulations.gov/comment/BIS-2024-0005-0026

[50] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

requirements for communications integration with surrounding infrastructure, cloud computing services and 'over-the-air' (OTA) software updates.

Consequently, passenger cars are now effectively internet-of-things devices. The EU is in the process of developing cybersecurity certification standards for IoT devices, based on the framework Cybersecurity Act and Cyber Resilience Act. However, a motor vehicle-specific regulatory framework for addressing data and physical safety concerns is already in place.

From July 2024, all new vehicles registered within the EU must be certified as compliant with UN Regulations 155 and 156, themselves based on ISO standards for cybersecurity engineering and software update engineering (hereafter abbreviated as R155/156). These require manufacturers to submit their management systems and products for audit against standards for organisational processes, responsibilities and governance, to mitigate risk associated with cyber threats.[51] Many European OEMs also require certification under the German-developed TISAX information security standard by suppliers of digital components and systems, including cloud computing providers for connected vehicles services, such as Amazon Web Services.[52]

For vehicles with level 3 (L3) automated driving capabilities ('conditional automation', with the vehicle able to make informed decisions based on environmental detection), EU legislation aligns with UN Regulation 157. Regarding cybersecurity and software updates, this requires compliance with R155/156, as well as identifiability of onboard software (through a standardised identification code, as defined in R156).[53] Vehicles are required to carry a Data Storage System for Automated Driving 'black box' which records, for example, activation of the automated driving system and traffic lane changes initiated by the system.[54]

Compliance assessments for R155/156/157 are performed by entities designated by national authorities: for example, TÜV SÜD is designated by Germany's motor vehicle authority (KBA) to conduct audits for "all activities required by the KBA for the type approval of fully automated vehicles".[55] Chinese OEMs selling in Europe comply with these requirements, with one Chinese brand ceasing to sell models in Europe from July 2024 due to inability to meet these certification requirements (an outcome also forced on some European OEMs, including Porsche). [56] Increasingly (as noted in the BYD case study below), these compliance assessments are performed by Chinese service providers working in partnership with TÜV SÜD and other

[51] https://www.vehicle-certification-agency.gov.uk/connected-and-automated-vehicles/cyber-security-and-software-updating/

[52] https://www.regulations.gov/comment/BIS-2024-0005-0020

[53] https://unece.org/sites/default/files/2022-05/ECE-TRANS-WP.29-2022-59r1e.pdf; https://unece.org/sites/default/files/2021-06/GRPE-83-27.pdf

[54] https://unece.org/media/press/368227

[55] https://www.autonomousvehicleinternational.com/news/german-federal-motor-authority-kba-turns-to-tuv-sud-for-autonomous-driving-expertise.html

[56] Schmidt Automotive Research (correspondence with author); https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/.

designated European entities. This is a risk factor if there are concerns about the political pressure or incentives that Chinese actors may be working under, as noted in this report's concluding recommendations.

Automated driving relies on supporting technologies that are not directly regulated by the EU but are standardised through global industry processes. For example, light imaging detection and ranging (LiDAR) is being developed to standards worked out through bodies such as the ISO, with Chinese actors being major players in these processes.[57] The leading LiDAR vendor, China's Hesai, obtained TISAX AL3 certification based on an assessment by TÜV SÜD that included inspecting Hesai's data centres and production facilities.[58]

Another key technology is so-called 'V2X' ('vehicle to everything') communication protocols for vehicles to share information with each other and their environment, notably traffic control infrastructure and traffic management networks. The two main V2X protocols are DSRC, which is based on Wi-Fi standards and dominates in automated driving deployments in the EU (where its adapted version is referred to as ITS-G5), and CV2X, which is based on cellular telecoms (3GPP) standards and dominates automated driving deployments in China.

Both these technology standards build in privacy-preserving features, for example "pseudonym certificates" that indicate a CV2X certificate holder's permissions rather than its identity.[59]

3.1.3 State-led development, technical standardization and implementation of ICVs in China

These global technical standards for defining ICV-related technologies, including their information security aspects, are linked to China's domestic standards-setting process. Chinese actors working on developing and implementing these technologies participate in collaborative international SDOs such as the 5G Automotive Association and International Telecommunications Union, and keep them informed about developments within China.[60]
Guidance for developing a Chinese system of standards for chips (semiconductors) for the automotive sector issued by MIIT in 2023 stresses coordination and compatibility with international standards, including through active participation in international processes.[61]

In 2016, China promulgated a recommended national technical standard 'Technical Specifications for Electric Vehicle Remote Service and Management Systems' (GB/T 32960).[62]

[57] https://www.ets-ind.com/info-detail/china-takes-the-lead-in-developing-global-standards-for-lidar-for-the-first-time
[58] https://equalocean.com/news/2023040619595
[59] https://www.regulations.gov/comment/BIS-2024-0005-0018
[60] https://5gaa.org/content/uploads/2022/10/C-V2X-standardisation-in-China.pdf; https://www.itu.int/en/ITU-T/extcoop/cits/Documents/Meeting-20230922-e-meeting/19_CCSA_TC10_status_report.pdf
[61] https://www.gov.cn/zhengce/zhengceku/202401/content_6924893.htm
[62] https://std.samr.gov.cn/gb/search/gbDetailed?id=71F772D81157D3A7E05397BE0A0AB82A

Based on this standard, a ‘National Monitoring and Management Platform for New Energy Vehicles (NEVs)’ was developed, which has been collecting and analysing data from all NEVs in China manufactured since 2017.[63] This is a multi-level system that feeds data to a national platform, although the head of the institute that developed this system has said that the goal of real time transmission is probably not always achieved, with enterprises filtering the data they send.[64] Based on GB/T 32960, the national platform has 61 indicators for each vehicle including location, operational trajectory, engine function, mileage etcetera, and can monitor wider infrastructural information such as charging heat maps.[65] European automakers have confirmed to journalists that their cars in China participate in this system.[66]

In 2020, MIIT issued the Intelligent Connected Vehicle Technology Roadmap 2.0, which sets out a vision and goals for development of ICV technology in China.[67] It sets the ambition that by 2031-2035, ICV sales in China will account for more than 50% of new vehicle sales, with C-V2X ‘basically universal’ in new cars. ICV development is to be integrated with that of traffic infrastructure and larger ‘smart city’ management systems.[68]

China is running a multi-city pilot project over 2024-2026 to implement 'vehicle-road cloud integration’.[69] Participating vehicles are equipped with C-V2X and digital identity certificate carriers.[70] The goals include building a multi-level (edge and regional) cloud computing platform to provide integrated and collaborative sensing and decision-making to vehicles; securing data connectivity between vehicles and road-side units; developing standards for cross-domain identification and recognition;[71] and forming a unified standards and testing system.[72]

Imposing unified development guidelines on industry may seem heavy handed, but it addresses recognised information security deficits in China’s automotive sector, especially for trust-based mutual authentication over cloud platforms.[73] According to one 2021 paper authored by staff at CATARC, a state-owned research institute for the automotive industry:

> … detection methods and evaluation standards of intelligent automotive network security have not yet achieved professional unification, the number of samples in vulnerability databases is low, and threat

[63] http://www.bitev.org.cn/a/48.html; https://www.gov.cn/xinwen/2018-07/29/content_5310143.htm
[64] https://mp.weixin.qq.com/s/YKln1HqQbyyskwk-Ermllw
[65] https://www.gov.cn/xinwen/2018-07/29/content_5310143.htm
[66] https://apnews.com/article/4a749a4211904784826b45e812cff4ca#
[67] https://www.gov.cn/xinwen/2020-11/19/content_5562464.htm
[68] http://www.evinchina.com/articleshow-23.html
[69] https://www.gov.cn/zhengce/zhengceku/202401/content_6926711.htm
[70] https://www.globenewswire.com/news-release/2024/08/08/2926669/0/en/Global-and-China-C-V2X-and-CVIS-Industry-Research-Report-2024-By-2034-C-V2X-will-Cover-100-of-National-Highways-and-75-of-Urban-Intersections.html
[71] https://www.gov.cn/zhengce/zhengceku/202401/content_6926711.htm
[72] http://www.xinhuanet.com/tech/20240712/96bc72b7aec64266bda1b95e8174c2d3/c.html
[73] https://www.cjwk.cn/journal/guidelinesDetails/1711991105903587328

> intelligence cannot be exchanged, making it impossible for vehicle manufacturers, parts suppliers and automotive networking service providers to verify safety and reliability...[74]

Chinese academic literature also recognises the tension between data security and data utilisation efficiency for ICVs, and the need for regulatory innovation in this area.[75] But Chinese industry, encouraged by industrial policy goals such as those described above, is not waiting on data regulation to forge ahead with ICVs and automated driving. One 2022 study of Chinese patent data using the keyword "intelligent vehicles" found the three dominant fields to be information communications and data processing, control components and systems, and navigation and positioning. The same paper estimated that from January to September 2022, sales in China of passenger vehicles with L2 and L2+ automated driving capabilities rose year-on-year by 49.1%, accounting for 28.1% of total sales - a higher penetration ratio than that for new energy (electric) vehicles over the same period.[76]

Standard-setting continues apace. In August 2024, the Standardization Administration of China promulgated three new mandatory national technical standards concerning ICVs. These are GB 44495-2024 Automobile Comprehensive Information Security Technical Requirements; GB 44496-2024 Automobile Software Upgrade General Technical Requirements; and GB 44497-2024 ICV Autonomous Driving and Data Recording Systems. MIIT's related press release described these as China's first mandatory ICV technical standards, and their development as being 'fully harmonized' with UN Regulations 155 and 156 and other international regulations.[77]

3.1.4 Case studies: BYD and Nio (Project Lion Cage)

BYD is by far the leading Chinese electric vehicle vendor by sales domestically and abroad, overtaking Tesla by global EV sales volume in Q4 2023.[78] It is the first OEM licensed in China (December 2023) to conduct vehicle testing with L3 automated driving capabilities.[79]

BYD's leading passenger car models by sales in Europe are the Atto 3, Dolphin and Seal.[80] The Yangwang U8 SUV and a smaller model, the Bao 5, will also be available in Europe during 2024.[81] BYD's successful certifications for R155/156 in the EU appear to have been handled by ATIC,[82] a

[74] https://www.atlantis-press.com/proceedings/icprss-21/125961632

[75] https://qikan.cqvip.com/Qikan/Article/Detail?id=7107144245&from=Qikan_Search_JournalSearch

[76] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4678511

[77] https://wap.miit.gov.cn/xwdt/gxdt/sjdt/art/2024/art_9fa0f052fe7d4a4683e366eb1afff952.html

[78] https://www.bbc.co.uk/news/business-67860232

[79] https://www.reuters.com/business/autos-transportation/byd-has-obtained-conditional-testing-license-level-3-autonomous-driving-high-2023-12-27/ https://www.reuters.com/business/autos-transportation/byd-has-obtained-conditional-testing-license-level-3-autonomous-driving-high-2023-12-27/

[80] SAR, Aug 2024, p16

[81] https://press.aboutamazon.com/2023/11/byd-selects-aws-to-accelerate-global-expansion

[82] https://www.atic-ts.com/atic-has-successfully-assisted-byd-to-obtain-isosae-21434-certificates-csmssums-certificates-and-un-r155156-vta-certificates-a-total-of-5-certificates/

Chinese testing and certifications provider whose Europe-based staff appear to work under designated technical service providers such as TÜV SÜD.[83]

BYD's builds it vehicles on a proprietary e-Platform 3.0 architecture,[84]which enables intelligent motion control (dynamic state recognition and image recognition), intelligent voice control and cloud services provided through a BYD app.[85] [86] The next architecture version (4.0) is expected to be launched in 2024 with increased component integration.[87] The U8 SUV comes with the option of an integrated drone developed in partnership with DJI, which appears to be a modified version of DJI's Mavic 3, designed for photography and video.[88]

BYD's vehicles use an electric powertrain integrating multiple components.[89] The 'brain' chip (vehicle control unit, VCU) for this system, which controls power domain functions such as battery regulation and charging, is likely to be designed and manufactured in-house by BYD. Independent analysts assess most of the powertrain's components to be manufactured or assembled by BYD.[90] The company produces its own microcontroller units (MCUs),[91] enabling electronic control of applications such as door locks and window opening.[92]

BYD's Android-based intelligent cockpit system (DiLink) enables functions that include navigation, voice recognition and control, and remote control of the vehicle through the BYD app over the cloud.[93] The company's latest Seal EV sedan model integrates LiDAR[94] provided by a Chinese vendor (RoboSense, part owned by BYD and Xiaomi, the latter a leader in IoT devices)[95] and features the "in-house developed DiPilot 300 assisted driving system, capable of point-to-point pilot-assisted driving on highways and urban roads."[96]

In May 2024, BYD Europe's CEO said the company uses Google Cloud and Orange (France) for connectivity services, and that "no data will transfer outside [Europe]... We don't use any Chinese platforms [...] to transfer our key data."**[97]** He further stated that the company's email service is

[83] https://www.atic-ts.com/european-vehicle-and-components-type-approval/

[84] https://www.byd.com/eu/blog/Why-is-BYDs-e-Platform-3-0-so-special.html

[85] https://carnewschina.com/2024/05/14/byds-e-platform-3-0-evo-has-five-major-tech-clusters/

[86] https://ev-database.org/uk/car/1919/BYD-DOLPHIN-604-kWh

[87] https://cnevpost.com/2024/03/11/byd-to-launch-next-gen-phev-bev-platforms-further-offensive-petrol-cars/

[88] https://www.heliguy.com/blogs/posts/store-and-deploy-your-drone-with-the-yangwang-u8-suoer-suv

[89] https://www.byd.com/eu/car/atto3

[90] https://www.yolegroup.com/technology-outlook/whats-in-the-box-byds-8-in-1-electrification-system-at-a-glance/

[91] https://www.maritex.com.pl/product/attachment/162842/73282dbfeeef6a6c68f3d32dc2f83beb (BYD specs datasheet, English Rev1.0 2021)（Chinese Rev 1.3 2021: https://www.bydmicro.com/params/field/preview/PDF_PRODUCT_202111015643.PDF)

[92] https://wap.seccw.com/document/detail/id/20774.html

[93] https://www.byd.com/sg/support/dilink

[94] https://cnevpost.com/2024/08/08/byd-launches-2025-seal-ev-07-dm-i/

[95] https://carnewschina.com/2024/08/02/new-byd-seal-ev-revealed-with-lidar-in-official-images

[96] https://cnevpost.com/2024/08/08/byd-launches-2025-seal-ev-07-dm-i/

[97] https://www.topgear.com/car-news/business/boss-chinese-carmaker-byd-has-addressed-european-drivers-data-protection-concerns

provided by Microsoft and its enterprise management software (handling manufacturing and shipment data) is provided by Germany's SAP. The memory solution for BYD's enterprise management system is provided by Huawei.[98]

BYD Europe's privacy policy[99] states that it "will not disclose Personal Data provided by Data Subjects to any party, other than BYD Europe itself, without prior permission from the Data Subjects." Transfers of personal data to a non-EU country "such as to China" will only take place in accordance with applicable laws, for example in line with GDPR standard contractual clauses. BYD Europe's website describes in-vehicle data protection features such as managing third-party software (for example, mapping apps) to require privacy policy disclosure and user choice in data processing, and data collection minimisation, for instance through user activation of the voice assistant (rather than this remaining active by default).[100]

BYD provides lifelong free OTA software updates.[101] These are delivered by Amazon Web Services (AWS) as a managed service, meaning that AWS has functional control of the process.[102] According to AWS:

> … BYD uses AWS capabilities to manage security for its vehicles, improve governance, and maintain regulatory compliance for its overseas connected vehicle platform. For example, BYD uses a broad set of AWS security, identity, and compliance services to achieve seven-layer protection for connected vehicles applications, guarding against common vulnerabilities and cyberattacks. … AWS provides… for BYD's core operations, including Amazon Simple Storage Service (Amazon S3), which stores vehicle system data…". [103]

Examples of vehicle features that can be enabled by OTA update include internet browsing through DiLink[104] and 'Navigation on Autopilot', allowing drivers to take their hands off the steering wheel for brief periods. The extent to which such automated driving features can be legally deployed in a given jurisdiction is governed by local legislation. EU legislation aligns with United Nations regulations on driving automation and provides for vehicle type approval for models with level 3 (L3) and, with more restrictions, level 4 (L4, fully driverless) systems.[105] The situation for L2 'hands free' driver assistance features such as 'navigation on autopilot' is more ambiguous, with EU regulatory approval granted on an exemption basis for certain systems, for example Ford's BlueCruise.[106]

[98] https://e.huawei.com/es/ict-insights/global/ict_insights/201810190908/manufacturing/201901191539

[99] https://www.byd.com/eu/privacy#2

[100] https://www.byd.com/en-qa/data-privacy

[101] https://www.byd.com/sg/support/dilink

[102] https://press.aboutamazon.com/2023/11/byd-selects-aws-to-accelerate-global-expansion

[103] https://press.aboutamazon.com/2023/11/byd-selects-aws-to-accelerate-global-expansion

[104] https://mb.com.ph/2024/7/22/byd-lets-you-check-on-your-car-with-your-phone

[105] https://single-market-economy.ec.europa.eu/sectors/automotive-industry/vehicle-safety-and-automatedconnected-vehicles_en

[106] https://www.autofutures.tv/topics/ford-bluecruise-hands-free-driving-technology-approved-for-use-across-europe-s-highways/s/d799a5c9-aef2-4fa4-97d7-b7bf5823e6b7

In line with the trend towards 'software-defined vehicles' and the enabling centralised computing architectures, next generation BYD models (and those of other Chinese OEMs) will use the DRIVE-Thor system-on-chip (SoC) provided by Nvidia, the US-based AI leader.[107] This single chip consolidates functions that previously were managed through distributed control units (parking, driver assist, instrument cluster, infotainment etc), isolating the relevant computing processes so that they can run concurrently without interruption.[108] DRIVE- also allows a vehicle to simultaneously run multiple operating systems (like Android and Linux).[109]

DRIVE-Thor is claimed to be the first automotive chip to use an inference transformer engine,[110] the technology behind generative AI applications like ChatGPT.[111] BYD also plans to use Nvidia's AI infrastructure for cloud-based AI development and training.[112] Generative AI is being employed by automotive OEMs to develop synthetic data for training autonomous driving systems designed to respond to and learn from users' prompts, requests, and driving styles, and to build enhanced vehicle safety systems based on large data sets.

Nvidia is co-developing automotive applications with Chinese technology vendors like Alibaba. The latter has already integrated its proprietary large language models (LLMs) with Nvidia's older DRIVE-Orin SoC. Alibaba and Nvidia recently announced they will integrate Alibaba's LLMs with DRIVE-Thor for such applications as advanced voice assistance (that will, for example, be able to offer dynamic driving recommendations).[113] Nvidia's DRIVE-series SoCs are open and modular platforms that run on Nvidia's DriveOS operating system, developed for automotive use to security standards certified by TÜV SÜD.[114]

In January 2024, BYD released its Xuanji AI-enabled intelligent architecture, described as "both brain and neutral network," implying that it controls vehicle functions as well as processing data. BYD claims that this system "perceives changes in the internal and external environment of the car in real-time [and] adjusts the state of the vehicle [accordingly]."[115]

It is described as edge-based as well as cloud-based, probably meaning that the vehicle's onboard AI capability can manage a range of trained scenarios without communicating with the cloud. The underlying AI model reportedly covers over 300 vehicular scenarios.[116]

While BYD will likely be the leading Chinese EV vendor in Western Europe, other Chinese OEMs have achieved notable sales. One ongoing open source project ('Lion Cage') by Norway-based

[107] https://nvidianews.nvidia.com/news/nvidia-drive-powers-next-generation-transportation
[108] https://blogs.nvidia.com/blog/drive-thor/
[109] https://venturebeat.com/ai/could-nvidias-thor-chip-rule-automotive-ai/
[110] https://blogs.nvidia.com/blog/drive-thor/
[111] https://nvidianews.nvidia.com/news/nvidia-drive-powers-next-generation-transportation
[112] https://nvidianews.nvidia.com/news/nvidia-drive-powers-next-generation-transportation
[113] https://www.scmp.com/tech/big-tech/article/3279428/alibaba-nvidia-collaborate-advanced-autonomous-driving-solution-computing-services
[114] https://developer.nvidia.com/drive/os
[115] https://www.byd.com/us/news-list/BYD-Showcased-Intelligence-Advancement-Dream-Day-2024.html
[116] https://autotech.news/byd-unveils-integrated-vehicle-intelligence/

researchers is investigating cybersecurity and data transfers using an ES8 sports utility vehicle BEV sold by Nio, one of the leading Chinese EV startups.[117]

The ES8 is a 2018 model vehicle that was launched in Norway in 2021. Like BYD, Nio's privacy policy states that personal data is stored within the EU, but may be "transferred to, and processed and stored in, countries… where we and our third-party service providers… have operations… including but not limited to [the] USA or China". Such extra-EU transfers are to be GDPR-compliant, for instance in accordance with standard contractual clauses.[118]

To date, notable findings by Project Lion Cage (concerning only one test vehicle) include:

- Of more than 200,000 DNS requests from the vehicle that were logged over a 7 month period, almost 90% went to servers in China, mostly associated with unencrypted HTTP GET requests that mainly related to the vehicle's map system making version checks (only 1 POST request was identified).

- Requests resolving to qq.com (associated with China's Tencent) were hosted on servers in Sweden that were owned by the US cloud computing provider Akamai. This was presumably done to comply with GDPR requirements (and potentially to enable data transfer with low latency by geographical proximity to the user), although without decrypting the data it was not possible to comment on the content involved. Other traffic was hosted by Amazon CloudFront on servers in North America.[119]

- Navigational routing was done by querying Amazon Web Services (AWS) servers in Germany. This was also the delivery mechanism for OTA updates (refer further comment on this below). Also based on the DNS queries, optimisation of these AWS services for Nio's European-based cloud appears to be managed by the US-based company Nautilus.[120]

- Most of the data traffic (90% of all requests) was accounted for by a single unencrypted file downloaded repeatedly from a Nio site hosted on a Tencent Cloud server in Beijing. This server supported SSL versions back to TLSv1.0, implying a poor level of security (TLSv.1.0 has been PCI non-compliant since June 2018).[121] The Lion Cage researchers did not reach a conclusion about the function of this file.

[117] https://www.linkedin.com/pulse/project-lion-cage-part-1-tor-indst%C3%B8y/

[118] https://policy.eu.nio.com/en_US/#/app-privacy

[119] https://www.linkedin.com/pulse/project-lion-cage-part-5-how-secure-vehicle-hosting-tor-indst%C3%B8y/

[120] https://www.linkedin.com/pulse/project-lion-cage-part-5-how-secure-vehicle-hosting-tor-indst%25C3%25B8y/

[121] https://www.linkedin.com/pulse/project-lion-cage-part-5-how-secure-vehicle-hosting-tor-indst%C3%B8y/

- The ES8's system on chip (SoC) was provided by a European vendor (Swiss-based U-Blox). Attempts to hack the vehicle through this SoC (using a sample device supplied by U-Blox) showed a high level of security, with 4137 requests only receiving back 1 data packet.[122]

- One data collecting feature that is not readily apparent to the user nor highlighted in Nio's marketing materials is a "smart visual system" for sensing the driver's concentration level. This appears to be enabled by a camera unobtrusively embedded in the rear view mirror. However, this system is mentioned in the ES8's user manual (available on the internet).[123]

- In at least one case, unencrypted data transmission resulted from EU regulatory requirements, specifically to include TPMS sensors with unique identifiers inside the tires that transmit to the vehicle its tires' pressure and temperature data as well as the sensor ID. This ID is non-randomised and so allows the individual vehicle to be tracked by external parties using basic commercial off-the-shelf equipment. This was also true for the vehicle's Bluetooth-enabled wireless key fob, although in this case the data transmitted was encrypted and well secured.[124]

- Regarding security inspection of data by cloud computing providers, specifically by AWS when delivering OTA updates, one of Lion Cage's researchers told this report's authors that the analysis showed it was unlikely that any code analysis was taking place.

As an interim conclusion based on these (very limited) case studies, vehicle models with automated driving features offered by Chinese OEMs in Europe do not seem to have glaring cyber or data security vulnerabilities. They meet technical compliance requirements, incorporate privacy preserving features and use components that meet high technical cybersecurity standards. Data transmission to and from the vehicles is provided by US and European cloud vendors. There are some data transmissions that are not malicious on their face but deserve further analysis and explanation from the Chinese OEM. Overall however, it is difficult to say based on technical features alone that there is a clear picture of cybersecurity risk linked to Chinese OEMs' vehicles, beyond what is common to products of this type regardless of vendor nationality. As noted in the conclusions at the end of this report, the risk linked to these vehicles depends on assessment of the political and regulatory pressure that might be exerted by Chinese authorities on Chinese OEMs, systems and components vendors, and service providers who conduct compliance certifications in Europe on delegated authority from European entities.

[122] https://www.linkedin.com/pulse/project-lion-cage-part-6-how-car-secured-can-anyone-tor-indst%25C3%25B8y/

[123] https://www.linkedin.com/pulse/beware-your-private-moments-car-tor-indst%C3%B8y-ialrf/

[124] https://www.linkedin.com/pulse/project-lion-cage-part-6-how-car-secured-can-anyone-tor-indst%25C3%25B8y

3.2 Chinese made and designed civil drones

3.2.1 UAV production and operational regulation in the EU and China

Civil UAV operation is governed by EU Regulations 2019/947 and 2019/945, which do not distinguish between recreational or commercial activities, instead providing a risk-based framework that differentiates by drone weight, specification and intended operational purpose.[125] From 1 January 2024, an active remote identification system (allowing the general public to identify the individual UAV) has been mandatory for a large range of drones.[126]

These regulations do not contain specific data privacy or cybersecurity provisions.[127] However the EU Cyber Resilience Act (CRA), which applies to 'products with digital elements' and so will likely cover UAVs (motor vehicles are excluded since they have their own sectoral cybersecurity regulation, described in the preceding case study), obliges manufacturers to conduct an organisational risk assessment and vet third-party component suppliers to ensure conformity with the CRA's cybersecurity requirements for products. These can be self-performed using certification schemes set out according to the EU Cybersecurity Act, but for certain product classes a third-party assessment is mandatory.[128]

Regarding UAV traffic management in the EU, the 'U-Space' concept of operations (ConOps)[129] sets out a set of procedures and services (for example, network identification, traffic information and conformance monitoring) and an organisational division of labour 'to support safe, efficient and secure access to airspace for large numbers of drones [based] on a high level of digitalisation and automation of functions.'[130] One recent gap analysis of the latest U-Space ConOps edition recommends *inter alia* an obligatory certification process to provide data on UAV performance characteristics, technological solutions for collecting data from UAVs operating within the U-Space system, user preference collection through an online software interface and AI-enabled security breakthrough and threat analysis, also noting that further study is required on fusing multiple-source sensor information for real-time use.[131]

Similar themes are apparent from China's production and operations governance for UAVs, which are described under 'Section Specific Regulation: Drone Data' above. In August 2022, the

[125] https://www.easa.europa.eu/en/domains/drones-air-mobility/rules-standards

[126] https://www.easa.europa.eu/en/document-library/general-publications/remote-identification-will-become-mandatory-drones-across

[127] https://www.osborneclarke.com/insights/drone-liability-age-ai-and-cybercrime-what-legal-framework

[128] https://www.osborneclarke.com/insights/drone-liability-age-ai-and-cybercrime-what-legal-framework

[129] https://op.europa.eu/en/publication-detail/-/publication/a822bdd4-c49e-11ee-95d9-01aa75ed71a1/language-en

[130] https://doi.org/10.2829/335092

[131] https://www.mdpi.com/2226-4310/11/6/471#:~:text=Selection%20among%20algorithms%20and%20software,with%20regulation%20or%20standardization%20requirements.

Civil Aviation Administration of China (CAAC) issued a Civil UAV Aviation Development Roadmap that outlines ambitions to upgrade the extant UOMS platform, that will combine 5G, AI and other advanced technologies to achieve traffic to move from isolated to integrated operation of UAVs, which will presumably take the form of the comprehensive UICSSP platform referenced in China's UAV Management Regulations and UAV Production Regulations.[132] Meanwhile, the extant UOMS platform allows CAAC to 'realise [for UAVs] the functions of controller management, registration management, airworthiness management, air traffic management, operation management, etc. and provide corresponding services.'[133]

China's extant UAV management system thus remains under centralised control by the government's general civil aviation authority, following the traditional model of air traffic management. Critical Chinese assessments of China's UAS traffic management system describe it as still technically primitive, equivalent to the primary level of drone management systems in the US and Europe. For instance, the services provided by China's civil UAV traffic management information service system (UTMISS), a pilot project that is being trialled in several locations including Shenzhen, Shanghai and Hainan, are described as only equivalent to the first (U1) level out of four levels of progressively increasing services outlined by the EU's U-Space ConOps.[134] If accurate, this would mean for example that UTMISS allows electronic registration of drones (U1) but not identification or tracking (U2).[135]

Additionally, in Hangzhou a third-party provider (Zhejiang Herefly Technology[136]) runs a separate developmental UAV management system, the UAV Operation Management Service Center.[137] Delegating service provision of UAV management functions to third parties (again with reference to the EU's U-Space ConOps) is recommended by some Chinese commentators to reduce the burden on the government to provide such services, and speed up progress towards meeting the technical requirements of UAV flight management.[138]

China's recent economic development emphasis on the 'low-altitude economy', which was referenced in the Chinese Communist Party's Third Plenum Resolution of July 2024,[139] adds to the imperative for rapid technical and regulatory innovation in this area. Progress in rolling out 'smart city' infrastructure also creates opportunities to leverage UAV operation for other urban management goals. For example, one 2023 study offers a framework to manage data hotspots

[132] http://www.caac.gov.cn/HDJL/YJZJ/202208/P020220822615871900321.pdf

[133] https://xxgk.mot.gov.cn/2020/gz/202401/W020240103570150577134.pdf

[134] https://www.7its.com/index.php?m=home&c=View&a=index&aid=23305 (rule 92.9, referring to the UOMS 民用无人驾驶航空器综合管理平台 as part of the UICSSP 国家无人驾驶航空器一体化综合监管服务平台)

[135] https://op.europa.eu/en/publication-detail/-/publication/a822bdd4-c49e-11ee-95d9-01aa75ed71a1/language-en

[136] https://en.chinaerospace.com/article/show/cb10ae009f72fd1bd712f970761c03ec

[137] https://www.hangzhou.gov.cn/art/2022/1/7/art_812266_59047581.html

[138] https://www.7its.com/index.php?m=home&c=View&a=index&aid=23305

[139] https://www.pekingnology.com/p/full-text-resolution-of-the-central

(overworked nodes in networks) through collaboration between drones and 5G edge computing, raising data processing efficiency and reducing energy consumption.[140]

3.2.2 Chinese civil drone vendors' presence in the EU

China's DJI (case study below) remains by far the largest vendor worldwide of commercial-off-the-shelf (COTS) drones, with a 2023 global market share of around 70%, based on a wide cross-sectoral enterprise product portfolio as well as its well-known recreational models. Another Chinese-headquartered company, Autel Robotics, has been significantly growing its market share.[141] Swiss-owned Yuneec is another large market player that manufactures in China.

In the electric vertical take-off and landing aircraft (eVTOLs) segment, i.e. larger drones designed for passenger or cargo transport, Chinese company EHang has engaged in some European testing initiatives. In late 2023, EHang obtained type certification from CAAC for a passenger UAV model (EH216-S), qualifying it for passenger-carrying UAV commercial operations. EHang's press release describes an extensive testing process for safety, airworthiness and functionality that included environmental tests, data link and ground control communications, and electromagnetic compatibility as well as flight performance and overall system functionality.[142] However CAAC's airworthiness certification process is reportedly considered opaque by foreign observers, and the specific design of the EH216-S is also reportedly likely to face challenges meeting airworthiness standards in Europe.[143]

Nonetheless in February 2024, EHang signed an agreement with Spain's Telefonica (providing 5G communications) to trial use cases for EHang's eVTOLs in passenger transport, logistics, healthcare and emergency response. The agreement included the intention to jointly "develop connectivity solutions based on mobile networks for… integration of drones and eVTOL aircraft with digital unmanned air traffic management systems".[144] EHang has also conducted test flights with the EH216-S under the SAMVA project, funded by the EU to test eVTOL implementations.[145] These flights were operated from EHang's Urban Air Mobility (UAM) centre, reportedly Europe's first, in a Spanish regional airport.[146]

3.2.3 Case study: DJI

While originally relying heavily on components from non-Chinese vendors, DJI appears to have steadily increased the ratio of Chinese-supplied and in-house designed components in its drones over the past half-decade, with the small number of foreign-made components that it does still incorporate in its models arguably being due to these being "best in class" rather than to the

[140] https://dl.acm.org/doi/10.1145/3617373

[141] https://dronelife.com/2023/06/13/droneii-drone-industry-investment-and-growth-from-the-floor-of-energy-drones-and-robotics-summit/

[142] https://www.ehang.com/news/990.html

[143] https://aerospaceamerica.aiaa.org/heres-why-you-might-not-see-those-ehang-air-taxis-outside-china-any-time-soon/

[144] https://www.mobileworldlive.com/telefonica/telefonica-inks-deal-with-flying-urban-vehicle-player/

[145] https://www.ehang.com/news/1097.html; https://www.samva-project.eu/about-3

[146] https://www.airport-technology.com/news/ehang-inaugurates-first-european-uam-center/?cf-view

absence of Chinese alternatives.[147] Greater reliance on Chinese component suppliers potentially reduces the insight that foreign observers have into these suppliers' information security credentials. One potential remediation from a European viewpoint would be for DJI to require component supplier certification according to trusted audit frameworks such as TISAX (described in the automotive sector case study above).

One teardown of DJI's Mavic Pro 3 - a 2023 model triple-camera drone for photography and videography, an adaptation of which is sold as an integrated unit with BYD's new model SUV (see case study above) - showed that the wireless/Bluetooth connectivity module was provided by Synaptics (US), memory (SDRAM) was provided by SK Hynix and Samsung (South Korea), but that the application processor, video processor and microcontroller unit[148] were likely provided by Chinese vendors LeadCore and HDSC (Huada).[149] The latter company is part of the state-owned CEC group, which is on the US Chinese Military Companies List,[150] while CEC Cloud is on the US Commerce Department's Entity List.[151]

DJI itself has for years been subject to scrutiny over the data security of its products. The company publishes online a 'drone security white paper' (latest version 3.0 released April 2024[152]) which discloses some details about its drones' wireless communications protocols (including its proprietary closed OTA protocol OcuSync), security features of its Android and iOS apps, cloud services including its cloud-based platform for fleet management (DJI FlightHub), and chip/hardware security. This document also describes DJI's 'bug bounty' program for security vulnerability reporting and summarises the results of multiple independent audits into the data and cybersecurity of its products.[153]

These audits have all been conducted by non-Chinese entities, among them US private sector firms (including Booze Allen Hamilton, a US Department of defence contractor) and the Idaho National Laboratory (commissioned by the US Department of Homeland Security).[154] While some of these audits have identified security vulnerabilities exposed to potential threat actors (which have then been remediated by DJI under the auditor's supervision), none have found unauthorised data transmission to unexpected parties.[155]

[147] https://fpvwiki.co.uk/dji-reliance-on-western-component-supply-to-manufacture-drones-truth-or-myth

[148] For example (not necessarily the Huada MCU in the Mavic 3 Pro): https://www.hqonline.com/product-detail/32-bit-mcu-microcontrollers-hdsc-hc32l136k8ta-2500304765?srsltid=AfmBOoqsHpvxTtLbEO4HPzIStnG6ywEH6cqUA7K1Yn3yVirQiJK1pGCe

[149] https://www.youtube.com/watch?v=R9Sg6q-0gK4

[150] https://www.akingump.com/en/insights/alerts/dod-updates-section-1260h-list-of-chinese-military-companies-operating-directly-or-indirectly-in-the-united-states

[151] https://www.federalregister.gov/documents/2022/12/19/2022-27151/additions-and-revisions-to-the-entity-list-and-conforming-removal-from-the-unverified-list

[152] https://www.dji.com/global/media-center/announcements/dji-launches-trust-center

[153] https://www.dji.com/global/trust-center/resource/white-paper

[154] https://www.auvsi.org/sites/default/files/DHS%20report.pdf

[155] https://www.heliguy.com/blogs/posts/no-evidence-of-drone-data-going-to-dji-or-china

Two 2022 audits of recreational[156] and enterprise[157] drone models and DJI's associated apps were conducted by Germany's TÜV SÜD (which as mentioned above, is designated to conduct the cybersecurity certifications for motor vehicles that are required by EU regulations).[158] One of the summary reports from TÜV SÜD states:

> [We] tested the aircraft in accordance with the cybersecurity standards established by the US National Institute of Standards and Technology (NIST) and European Telecommunications Standards Institute (ETSI), as well as the industry-recognized Open Web Application Security Project (OWASP) Mobile Application Security, and the Penetration Testing Execution Standard (PTES).
>
> [...]
>
> DJI drones have comprehensive security features based on standards of practice, and the sensitive information in the communication process of App DJI Fly v1.5.10 (iOS & Android), as well as the cloud flight data synchronization process of DJI drones, are both encrypted and transmitted through SSL, which can avoid most common security risks. The cybersecurity capabilities and privacy protection aspects of DJI drones meet the requirements of NIST IR 8259 and ETSI EN 303645 standards covered by this test.[159]

One 2018 audit of DJI products did find that DJI's Android and iOS apps made DNS queries to servers in mainland China and Hong Kong apparently hosted by Tencent and DJI (as well as to US-based AWS and Alibaba servers). The same audit found that user-initiated flight log uploads were sent in "non-encoded, plaintext form". However, the audit's general conclusion was that "users have control over the types of data DJI drones collect, store and transmit".[160]

According to DJI's current data storage and security statement:

> Data of international users collected by DJI is stored on best-in-class servers located in the United States. For the majority of this data, we use Amazon Web Services (AWS). The only data stored elsewhere are multimedia files users voluntarily upload to DJI's social media sharing forum SkyPixel. This data gets stored on Alibaba Cloud servers, which are also located in the U.S.
>
> DJI collects (app performance data and drone flight data including average number of pictures taken per flight) in aggregate and cannot identify individual users or use patterns from it. Users may deactivate transmission of this data in the settings menu of the DJI consumer flight control app.
>
> Location data is used to update nearby geofencing information [...] to protect the privacy of the operator's precise location, the DJI consumer flight control app applies a random offset of as much as 10 kilometres before transmitting Location Check Data to DJI**.** Location Check Data sharing cannot be deactivated in the DJI consumer flight control app.
>
> Photography/Videography Data [...] is never shared with DJI unless you manually turn on the sharing feature in the app.
>
> Flight Log Data [...] will only be shared with DJI if you manually use the "Sync" button on the DJI consumer flight control app interface.[161]

[156] https://sec-cdn.dbeta.me/djisrc/public/img/TUV-ETR-Comsumer.477de70.png

[157] https://sec-cdn.dbeta.me/djisrc/public/img/TUV-ETR-Industry.f3b9c92.png

[158] https://www.autonomousvehicleinternational.com/news/german-federal-motor-authority-kba-turns-to-tuv-sud-for-autonomous-driving-expertise.html

[159] https://dronedj.com/2022/12/01/dji-drone-cybersecurity-privacy-risk/

[160] https://www.theregister.com/2018/04/25/dji_data_security_audit/

[161] https://security.dji.com/data/consumer/

4. Conclusion and recommendations

4.1 Findings

The risks arising from the potential application of Chinese data legislation to acquire data pertaining to Dutch individuals through SCVs and drones divide into two categories. Where personal information (through the PIPL and subordinate regulations) is concerned, the risk is negligible. The PIPL is only applicable within China, with a limited scope of extraterritorial applicability that does not cover commercial products offered on European markets. Where the Data Security Law is concerned, residual questions arise over the obligation that data handlers must turn over data upon request. Specifically, the law is relatively silent on the circumstances that would trigger such an event, and the procedure that would need to be followed.

Risks arising from the National Intelligence Law cannot be understood in purely legalistic terms. On the one hand, the wording of the Law suggests that companies or individuals cannot be coerced to break the law in order to collaborate with intelligence services. However, the law is silent on whether that would include foreign legislation. Furthermore, while the law does provide for a possibility to file complaints, in the end, Chinese intelligence services face few meaningful independent legal or judicial constraints on their actions. Nevertheless, they do face political constraints. As such, the extent to which manufacturers of smart vehicles and drones could be subject to coerced collaboration depends on both cost-benefit calculations between the economic and security wings of the Party-state spectrum, as well as the technical facility or difficulty of doing so in a manner that achieves the aim of intelligence services while minimising the chance of detection. With regard to vulnerability processes under the Cybersecurity Law, insufficient public information is available to determine the degree of risks to Dutch data.

While assessing this balance, it needs to be borne in mind that Chinese authorities have taken data security in relation to smart devices, including vehicles and drones, very seriously. As a result, if such vehicles comply with Chinese regulations and applicable technical standards, they should already be very robust to the risks that attract concern from European policymakers by design.

It also bears remembering that Chinese technocratic governance practices in the vehicle and drone sectors align with international standards and practices. For instance, China's development plan for the automotive sector is pushing forward intelligentization and networking (including integration with roadside infrastructure and larger urban management systems) rapidly. The technological standards for this process remain linked to international standards development processes and collaboration with foreign actors. Governance of drone traffic management remains centralised in China's civil aviation authorities in line with traditional air traffic control models, although supporting services remain at a low level of development.

Furthermore, not all Chinese products are exclusively "Chinese". The BYD case study shows that many of the brand's data-related components and services, including cloud-based data management services and onboard computer processing, are provided by non-Chinese vendors in Europe or the US (e.g. AWS and Nvidia). Their products also comply with EU cybersecurity certification requirements as verified repeatedly by well-respected European homologation and certification bodies on the basis of existing international standards. BYD vehicles are advertised to contain privacy-protecting features that prioritise user control over data collection, and the company's privacy policy states that user data is stored in the EU and only transferred to non-EU countries (including China) in compliance with the GDPR.

Similar results are shown by the analysis done by the open source Project Lion Cage for a specific vehicle model that is described in the Nio case study. But the Lion Cage analysis also showed data transmission vulnerabilities that could be easily exploited by external parties, and data collection features beyond what was highlighted to the vehicle's purchasers. However, in all cases these could be characterised as engineering or privacy management deficiencies rather than malicious design. The analysis also showed some data transmission by the vehicle to servers in China for purposes not always readily explicable. One of Lion Cage's researchers put it to this report's authors that based on the apparent lack of data inspection by AWS, Chinese security services could insert their own code into OTA updates without the knowledge of either the Chinese OEM or of AWS.

Regarding commercial drones, there are fewer global technical standards and regulations than in the automotive sector. Multiple independent audits by reputable US and European-based entities of drone models supplied by the leading Chinese vendor DJI have failed to discover significant "red flags" concerning unauthorised data transmission or cybersecurity backdoors, although data transmission to servers in China has sometimes been identified (and subsequently remediated under the auditor's supervision). Similar to Chinese OEMs' vehicles,, DJI products contain privacy-protecting features that prioritise user control over data. China's civil UAV flight management system remains a work in progress that appears to be lagging US and European equivalents in capabilities, and does not seem as yet to be decentralising functions to Chinese companies, but rather centralises them in the civil aviation authority.

The evidence currently available in public suggests that Chinese ICV and drone vendors make products that meet international security standards (as increasingly is required by the Chinese state) and comply with EU regulations, and generally have high quality data and cybersecurity features. Much of the computing and telecoms hardware and software in these products (including next-generation models) is provided by US and European firms, and data appears to be stored and processed by US and European firms within the EU, although in some cases data transmission to servers in China has been identified. In theory, these products' origin from China and Chinese firms may increase their data and cybersecurity risk profile for political reasons. But their observed vulnerabilities are typical of such products regardless of vendor nationality, and so fall within the imperative to address vulnerabilities industry-wide.

4.2 Recommendations

While the risks associated with data espionage and surveillance through smart vehicles and drones originating from China are relatively limited, there are still several measures policymakers and regulators could undertake to enhance their ability to assess and mitigate potential concerns.

- With regard to the unclarity of Chinese laws, including the Data Security Law and the National Intelligence Law, diplomatic engagement could be undertaken, to obtain greater insight or assurances from Chinese authorities on how such laws will and will not be applied.

- Within Europe, greater clarity is necessary on how the provisions of legislation such as the GDPR and the Data Act apply to specific products (for instance, it remains unclear exactly what constitutes personal data in relation to smart vehicles). This may require secondary legislation.

- Regulators should maintain as a default position that compliance with R155/156/157, i.e. the extant EU-wide cybersecurity requirements for all new motor vehicles registered as of July 2024, is satisfactory regardless of the nationality of the OEM (car manufacturer), while ensuring that these cybersecurity requirements, or related secondary legislation, is updated timely in response to technological developments.

- They should also maintain the general principle that where products comply with EU data and cybersecurity regulations as demonstrated through independent audits, further regulatory intervention for specific companies/brands/products should be based on risk factors demonstrated by product analysis (e.g. cybersecurity testing), not on political factors such as the nationality of the OEM or component vendors.

- Concerns about risks that stem from China's political and regulatory environment, and the pressure that Chinese authorities may bring to bear on Chinese OEMs, suppliers and service providers, should be addressed based on assessments of individual brands and vehicle or drone models, as exceptions to the general regulatory framework. In the authors' view, the limited evidence surveyed above does not support the conclusion that a separate regulatory framework (or complete ban) for Chinese-made vehicles in Europe is justified on data or cybersecurity grounds.

- The recommendations below that refer to Chinese vendors are offered in this context. They assume that a given Chinese OEM and/or vehicle model has raised sufficient concerns for European authorities to justify measures additional to the general regulatory requirements. By the same token, these recommendations could also be applied to non-Chinese vendors in the interests of raising the general level of security around connected vehicles and drones, regardless of vendor nationality.

- To mitigate concerns about the integrity of compliance testing done by independent technical services, national regulators could be given the authority to perform or re-do certain tests (for example, cyber penetration testing). Regulatory authorities would need to be adequately resourced for this purpose, in order to have the necessary technical knowledge and capacity to conduct such testing themselves.

- Ensure that international standards and homologation frameworks, such as EU regulation adopting UN R155/156/157, as well as the European homologation framework for automated driving, are updated timely in response to new technological developments, and remain fit for purpose.

- Regulators should consider the application of specific rules for sensitive areas and applications. For drones, it is already the case that European nations have instituted “no fly zones”. Similarly, regulations could mandate that certain vehicle sensors are disabled when entering sensitive zones such as proximity to military or government facilities. Vehicles acquired for purposes such as the transportation of senior government or corporate officials could also be subject to dedicated requirements, with corresponding guidance issued for private vehicle purchases by such individuals.

- Regulators should seek to better understand the importance of third-party component and service providers. To that end, they could, for example, engage with cloud and computing services providers used by Chinese automotive and drone OEMs in Europe (Amazon Web Services, Nvidia) to gain insights into their relationship with Chinese OEM customers, product integration with Chinese software providers (for example AI vendors like Alibaba), data handling for these customers and trends regarding information processing and data handling for ‘software-defined vehicles’.

- Regulators could also consider requiring Chinese OEMs to impose security audit requirements on their component suppliers (e.g. TISAX for the automotive sector). Increased Chinese component content (especially notable in the case studies of BYD and DJI but applicable for Chinese OEMs across the automotive and UAV sectors) increases the challenge of mitigating risk associated specifically with Chinese actors. Imposing audit requirements for component suppliers could be one potential mitigation pathway.

- To better understand ongoing auditing processes of Chinese vehicles, regulators could liaise with technical services providers designated to conduct cybersecurity certifications under the relevant frameworks (R155/156, ISO/SAE 21434) in Europe.

- Regulators could conduct manual audits of individual models from Chinese OEMs to verify their claims about installed privacy protection features and their functioning.

- With ICVs moving towards centralised compute architectures, regulators could consider mandating control redundancies in vehicle design, for example isolated manual control functions, in case accidental or malicious software failure degrades the functioning of digital control functions.

- Consideration could be given to empowering EU or member-state regulators to demand further technical information about vehicle components and systems, including chipsets and software code. Care should be taken that such legislation does not violate intellectual property and international trade laws. This should put the onus on proponents of such intervention to demonstrate why such product-specific information is necessary to mitigate particular risk profiles.

- Another option is adapting regulation to reduce the legal risk to ‘white hat’ hackers and so increase their willingness to engage in legitimate cybersecurity penetration testing, thus increasing the testing services pool and the likelihood that vulnerabilities are identified. This was recommended specifically in the case of extant German legislation by the German Automotive Industry Association in an August 2024 report.[162]

[162] https://www.vda.de/dam/jcr:feb32ffd-f195-45b4-9141-d3a01873c4f0/VDA-position-cybersecurity-tests.pdf?mode=view