Written evidence submitted by the NCC Group (SDV0011)

Introduction

NCC Group is delighted to have the opportunity to engage with the Transport Committee and offer our expertise as a UK-headquartered global cyber security and software resilience business.

NCC Group's mission is to make the world safer and more secure. We are trusted by more than 14,000 customers worldwide – including some of the largest firms in the automotive industry – to help protect their operations from ever-changing cyber threats. Indeed, we have a dedicated Transport Practice whose Global Director regularly shares his views and insights into emerging and future risks and opportunities[1], while, as a leading expert in this space, NCC Group's Senior Security Consultant Dr Liz James serves as Vice-Chair of techUK's Intelligent Mobility and Transport Steering Board. Recognising the increasing convergence of cyber security and safety in the connected world (which we explore in more detail below), we recently announced the acquisition of Adelard – a well-established UK computer system safety advisory business – extending our risk management service offering in the field of safety critical systems. In support of our mission, we continually invest in research and innovation as an intrinsic part of our business model to match the rapidly evolving and complex digital environment. Indeed, in FY2021, we delivered 3,400 research days. **The security of connected technologies is one of our core research specialisms.** For example, earlier this year, our researchers identified a vulnerability in Bluetooth Low Energy (BLE) used by cars with keyless entry, which would enable hackers to unlock, start and drive a vehicle using cheap off-the-shelf hardware[2]. We have also published a white paper on the cyber threats facing the connected car and intelligent transport ecosystem[3]; and have **many years' experience researching the safety and security of smart cities**, working with leading UK universities to understand how we architect, implement and operate smart city designs that are secure by design and safe.

We are passionate about sharing our expertise and insights with policymakers and parliamentarians who are tackling crucially important questions about the use of critical and emerging technologies. In this submission, we have focused on the safety and security of connected and automated vehicles, and the

underpinning regulatory framework, and hope that our input proves useful. Indeed, we would be delighted to give oral evidence to the Committee's inquiry to help explore the proposals we raise in this submission in more detail.

Definitions

We believe that some confusion has arisen around what constitutes "self-driving", "automated", "autonomous" and "connected" vehicles. So as to aid clarity, we define these terms below:

- **Automated vehicles:** A general term used to describe vehicles which can drive themselves without being controlled or monitored by an individual for at least part of a journey. The Society of Automotive Engineers International (SAE) has established six "levels" of driving automation[4], which, at a high level, describe the extent to which a vehicle's driving automation system performs dynamic driving tasks[5] on a sustained basis. They are:
    - Level 0 (no driving automation)
    - Level 1 (driver assistance) – e.g. adaptive cruise control
    - Level 2 (partial driving automation) – e.g. advance driver assistance systems such as parking assist and automatic emergency braking
    - Level 3 (conditional driving automation) – equipped with environmental detection capabilities and can make informed decisions for themselves, such as accelerating past a slow-moving vehicle
    - Level 4 (high driving automation) – does not require human interaction in most circumstances, with human manual override e.g. Waymo's self-driving taxi[6]
    - Level 5 (full driving automation)

- **Autonomous vehicles:** Autonomous vehicles and automated vehicles are often conflated. We suggest that autonomous vehicles should be considered Level 5 automated vehicles under the SAE taxonomy framework, whereby a vehicle does not require human attention at any time to drive the vehicle. Such vehicles will not be readily available for at least a decade, and would expect their ultimate deployment to be

accompanied by potential changes in ownership models, primarily from private ownership towards fleet management or Transport-as-a-Service (TaaS) models.

- **Connected vehicles:** A vehicle equipped with wireless communications technology that enables data transfer with other vehicles, infrastructure, or other networks. All new cars have a degree of connectivity.

- **Self-driving vehicles:** The SAE define self-driving as the full function of the dynamic driving task, performed by an automated driving system within its operational design domain. In other words, when the automated driving system is engaged, the human in the driving seat would no longer be responsible for the dynamic driving task. On SAE's levels of driving automation, self-driving vehicles would be considered Level 4 and above.

For the purposes of this inquiry, the main distinction to establish is between automated vehicles and connected vehicles. While the two are heavily intertwined – indeed, many driving automation systems rely upon the connectivity of the vehicle – and will likely evolve in tandem, the risk profile for each is different and should be considered as such.

Risk landscape

New vehicles can contain hundreds of millions of lines of code, and often, over a hundred embedded computer systems from many different automotive suppliers. This means if devices within the network of a connected vehicle have been poorly designed or are misconfigured, they can be attacked by threat actors, and there are many different wired and wireless entry points into the ecosystem that attackers can exploit. **The increasing complexity of connected vehicles, as companies incorporate new technologies, means that the attack surface is growing**, with connected vehicles targeted in three primary ways:

- **Data breach:** Threat actors can access a wealth of sensitive information – e.g. personal data in infotainment systems – or mount industrial espionage attacks to gain access to intellectual property, stored on other specialist embedded computers.

- **Safety:** Connected vehicles present very real safety risks. If hackers access safety-critical components such as steering, braking, acceleration or airbag deployment, or the components that control these, this could potentially result in injury or death. The automation of vehicles further complicates the safety risk landscape, as malicious actors can take control of driving automation systems, potentially without drivers and operators realising. As such, strong cyber security should be seen as a prerequisite to safety because, ultimately, we cannot make assurances about the safety of systems that we do not control.

- **Ransomware:** This would likely involve displaying messages on the screens of connected vehicles, convincing the driver that hackers have taken control of the vehicle's safety-critical systems (even if this is false) and demanding money to restore the safety of the vehicle.

Considerations for a regulatory framework

Public trust is fundamental to the successful rollout of connected and automated vehicles, but this trust could be easily undermined if cyber security is not prioritised. However, the diverse nature of the automotive industry – from small electric vehicle start-ups to huge multinational manufacturing groups and many other shapes and sizes of organisation in between – means that cyber security has had different priorities in different companies historically. This is especially due to the tight margins within the sector. A recent industry report highlighted that 30% of car manufacturers and suppliers do not have an established product cyber security programme or team[7]. As such, **we strongly advocate regulatory intervention to set minimum mandatory standards that vehicle manufacturers, software developers and other supply chain partners must abide by**. UN Regulations already exist on cyber security[8], software update management[9] and automated lane keeping systems[10], laying the foundations for outcome-focused regulation of connected and automated vehicles' design and development lifecycle which UK (and international) policymakers should look to build on. In doing so, the UK Government should promote a **holistic, agile and proportionate approach** to security and risk management that:

- **Establishes the roles and responsibilities of the various actors that play a part in a connected and automated vehicle's supply chain and lifecycle.** Who is responsible for the safety and security of a connected and automated vehicle? Is it the manufacturer, the software developer, the current owner of the vehicle, the previous owner of the vehicle, the MOT provider? What level of responsibility do the developers, owners and operators of connected systems (e.g. smart traffic lights; mobile phones) that will interact with the vehicle have? The lines of responsibility are often blurred, meaning that, in our experience, no one party takes ownership of the security/risk of a system. The assumption that another organisation in the supply chain is responsible for ensuring a system is secure and resilient is – in our experience – commonplace (but ineffective), and further clarity is needed.

- **Defines the UK's risk appetite**. Connected and automated vehicles will never be zero risk if we wish to pioneer their development, and crucially, deployment. As such, the UK should define its risk appetite so the red lines with regards to connected and automated vehicles and their security, safety and resilience are known.

- **Encourages organisations to move beyond a 'tick-box' approach to compliance toward embedding a true understanding of the cyber security and safety risks** presented by connected and automated vehicles, promoting continuous mitigation throughout the product design, development, and post-market lifecycle. This should include the development of technical guidance and mandated **regular and independent assessments** of vehicles' real-world resilience and ability to withstand incidents and shocks across the technology ecosystem. Further, we should not reinvent the wheel. There are already a myriad of existing regulations, standards and frameworks that can be built upon. These include (but are certainly not limited to) the aforementioned UN Regulations, as well as ISO/SAE 21434. Going forward, as connected and automated vehicles become an increasingly embedded part of the UK's road infrastructure, there will also be questions as to whether the vehicles (and/or the manufacturers of these vehicles) should be formally considered critical national infrastructure (CNI) (and therefore subject to

the same security regulations as other CNI such as the Security of Network and Information Systems (NIS) framework).

- **Aligns with other core regulatory regimes aimed at managing safety and security in a connected world.** Connected vehicles do not operate in isolation; rather, they form part of the cyber-physical infrastructure that is increasingly prevalent in daily life, from smart cities and smart road infrastructure to electric vehicle charging and mobile and other consumer devices that interact with vehicles (e.g. for the purposes of keyless driving, or, perhaps in future, to help identify pedestrians and other road hazards). The Government is regulating to embed 'secure by design' principles and best practice cyber security and safety assurance across the connected world, including but not limited to mobile apps, consumer connected devices, smart cities, electric vehicle charging, and other smart energy devices. In doing so, it must take a holistic view of the connected world, and consider how each regulatory regime will interact with one another.

- **Equips the UK's vehicle certification agencies with the resources and skills** to effectively enforce the adoption of safety and security standards. While there have been efforts to upskill agencies' workforce, there remains a significant cyber security skills gap across the agencies which will only get worse as automotive technologies evolve. In the short term, the Government should consider whether drawing in external expertise is needed to plug the skills gap.

- **Keeps pace with modern technological and societal developments** by building in flexibility, agility and periodic regulatory and legislative reviews from the outset and investing in coordinating and improving horizon-scanning. This ideally should include requirements for regulators and policymakers to engage regularly with innovation centres and industry experts.

- **Ensures vehicle drivers are equipped with the knowledge and skills they need to operate increasing automated and connected vehicles**, through updates to the UK driving test.

- **Considers how new and evolving vehicle technologies will interact with legacy vehicles and other road users** that will continue to be present on the UK's roads for the foreseeable future, building a regulatory regime that is inclusive of all road users.

People and skills

To ensure that connected and automated vehicles are secure by design, it is critical that those who design and build vehicles, such as engineers and software developers, bake in security considerations from the outset. However, in reality, these individuals do not always have the skills or understanding required to do this. At a base-level, **relevant engineering and software development educational programmes should reflect cyber security as part of the system development process**. In addition, **there is a need to develop specialists who are able bridge the gap between the design and development of a vehicle and good cyber security practice**. This should, we believe, be pursued through one or more appropriate Government-appointed bodies, such as the Engineering Council and the UK Cyber Security Council – the new standards-setting body for the cyber security industry which is developing career specialisms as part of its approach to tackling the cyber security skills gap.

Wider legislative framework

Security vulnerability research plays a critical role in ensuring the cyber security (and, as we have outlined, the safety) of connected vehicles. This is where cyber security researchers identify vulnerabilities in products and work with manufacturers and vendors to fix them, before malicious actors are able to exploit them for nefarious purposes. For example, where NCC Group's researchers identified the aforementioned vulnerability in Bluetooth Low Energy (BLE), before issuing the research publicly, we responsibly disclosed the details of the products tested to the manufacturers (including Tesla) and discussed mitigation approaches with the Bluetooth Special Interest Group (SIG). The UK Government recognises the important role vulnerability research plays – for example, the Product Security and Telecoms Infrastructure Bill will mandate that manufacturers of consumer connected devices must have a

vulnerability disclosure policy in place, that enables researchers to report these vulnerabilities. However, the Computer Misuse Act 1990, which was written over three decades ago and remains the primary law governing cybercrime in the UK, inadvertently criminalises a significant proportion of the type of vulnerability research cyber security professionals are capable of carrying out. This is because the Act, as it is currently written, blanketly prohibits all unauthorised access to computer material, irrespective of intent or motive. It means that researchers can face legal action for reporting a vulnerability to an organisation, even if the affected organisation has a vulnerability disclosure policy in place. We believe this undermines the government's aims to encourage greater vulnerability reporting, and that it should take a more holistic look at its cyber security laws and policy to ensure that they are fit for purpose. Specifically, **the Computer Misuse Act should be updated to include a statutory defence – as a matter of urgency – to put in law a basis from which cyber security researchers can defend themselves where they undertake legitimate cyber security activities.**

Working globally

Notwithstanding that the UK has geographically-specific and road design factors automated vehicle technology will need to consider and account for, the UK should **avoid creating domestic cyber security regulations that are not aligned to international standards**. Given the size of the UK market, and the ever-increasing complexity of international supply chains, divergence from global standards is likely to create unnecessary administrative burdens for organisations as they seek to navigate differing regimes and put the UK at a competitive disadvantage. Instead, the UK should be at the forefront of the standardisation of connected and automated vehicles globally, particularly given the risks associated with the proliferation of insecure components imported from (e.g.) China which could undermine the integrity of systems/vehicles. In addition, driving global standards creates opportunities for UK-developed and protected intellectual property to be adopted, and ensures interoperability across the global supply chain.

August 2022

Endnotes

[1] E.g. https://www.mynewsdesk.com/nccgroup/blog_posts/securing-the-connected-cars-of-the-future-102275
[2] Find more information here: NCC Group uncovers Bluetooth Low Energy (BLE) vulnerability that puts millions of cars, mobile devices and locking systems at risk | NCC Group Newsroom (mynewsdesk.com), or watch the exploit in action here on a Tesla Model Y: (161) Hacking group demonstrates Teslas can be unlocked remotely by relaying bluetooth from phone - YouTube
[3] latest-threats-to-the-connected-car-and-intelligent-transport-ecosystem.pdf (nccgroup.com)
[4] J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International
[5] Real-time operational and tactical functions required to operate a vehicle safely in on-road traffic.
[6] Waymo unveils self-driving taxi service in Arizona for paying customers | Reuters
[7] https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf
[8] UN Regulation No. 155 - Cyber security and cyber security management system | UNECE
[9] UN Regulation No. 156 - Software update and software update management system | UNECE
[10] UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS) | UNECE