# Crime Facilitated by Connected and Autonomous Vehicles (CAVs)

This briefing identifies 28 crime threats that may be facilitated by CAVs in the future and suggests approaches to addressing them.


## Summary

Connected and Autonomous Vehicles integrate advanced communication and autonomous driving technologies, enabling them to operate independently or with minimal human intervention. Despite the anticipated benefits for transportation, CAVs could be vulnerable to a wide variety of crimes unless security and crime prevention measures are proactively integrated into the technologies enabling their operation. This briefing examines the cybersecurity and crime threats that could be facilitated by CAVs – as identified in the literature and by experts – discusses existing approaches to prevent them and recommends actions to mitigate future threats.


## Introduction

Over the past decade, there has been a surge in innovation focused on the development of Connected and Autonomous Vehicles (CAVs) that can operate without human intervention. CAVs are expected to bring substantial benefits to society including increasing mobility for those with disabilities, improving the productivity of human drivers (e.g. allowing them to work, socialise or sleep during journeys), reducing accidents caused by human drivers, reducing energy consumption and emissions, and reducing road congestion. Economic benefits include the creation of new jobs in automotive manufacturing (SMNT, 2017). According to the UK Government, by 2035 40% of new cars sold in the UK could have autonomous capabilities.

The widely accepted SAE International standard J3016 defines six levels of automation:

**Level 0:** No driving automation
**Levels 1-2:** Driver assistance including lane assistance
**Levels 3-4:** Vehicle automation, but human intervention required in some circumstances
**Level 5:** Full driving automation (no human intervention)

In this policy briefing, we define CAVs as ground civilian vehicles with connectivity and/or automation at levels 3-5. These vehicles use a wide variety of communication and sensor technologies to detect and recognise objects and make informed decisions related to the vehicle's surroundings. The intelligence that underpins driving decisions is achieved by advanced data analytics such as machine learning and other artificial intelligence techniques, which allow the vehicle to detect and recognise objects, assess driving conditions, consider alternatives, and make appropriate driving decisions.

## CAV technologies

A variety of technologies are required to enable CAVs to achieve the levels of automation described above, including:

***Sensors*** – such as Light Detection and Ranging (LiDAR), ultrasonic sensors, radar, Global Navigation Satellite Systems (GNSS) and cameras, which enable CAVs to perceive their environment and support navigation and safety.

***Physical ports*** – including electric charging and data transfer ports, which are used to charge the vehicle, send or receive data, and complete diagnostics.

***Infotainment systems*** – use technologies like Bluetooth, smartphone integration, and (touch) screens to deliver multimedia content, navigation, and connectivity features.

***Human Machine Interface (HMI)*** *technologies* – include touchscreens, voice recognition, and biometric systems that facilitate user interaction with the vehicle.

***Data storage and monitoring systems*** – store the extensive data, including sensor readings and operational metrics, generated by CAVs, which are used for maintenance, safety, and regulatory compliance.

***Communication networks*** – play an important role by enabling communication between internal components of the vehicle (e.g. between Electric Control Units (ECUs) which manage vehicle functions), and vehicle to everything (V2X) communication which enables CAVs to communicate with their external environment to assist with route planning, safety, efficiency and other tasks.

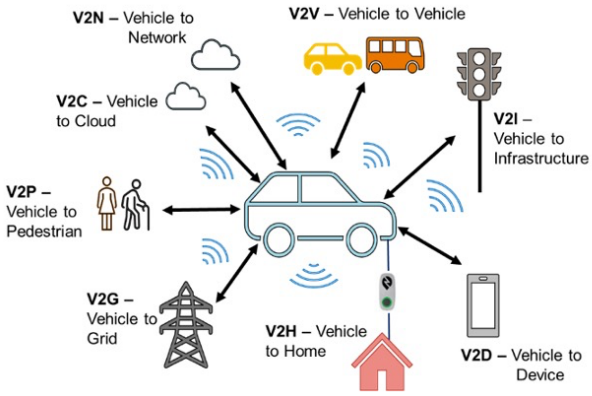


*Figure 1 Vehicle to everything (V2X) communication*

## Cybersecurity Threats

The complexity of CAVs means that numerous potential cybersecurity vulnerabilities exist. In this subsection, we discuss some of the "types" of threats identified in the literature and provide illustrative examples. It is important to note that not all attacks have been observed in the real-world, but they are nevertheless plausible. Some, but not all of these cybersecurity threats, will facilitate crime that is not limited to computer misuse (see next section). For each case, the numbers in parentheses show the total number of attack types identified in the literature.

Attacks against vehicle communication network systems (88 attacks): V2X communications are fundamental enabling technology for CAVs to operate safely and efficiently. Perhaps unsurprisingly then, one type of attack, commonly discussed in the literature involves the Denial of Service (DoS), for which an attacker sends large amounts of data to disrupt or degrade V2X networks. Other attacks include *Man-in-the-Middle attacks*, where an attacker intercepts data being communicated to either delay, manipulate or delete it, and *masquerading attacks,* for which a malicious vehicle pretends to be another vehicle.

Attacks against intra-vehicle communication systems (20 attacks): include those against the Controller Area Network (CAN) bus, which enables ECUs to communicate with each other, and for which security is weak. For example, *rogue update attacks* can be used to update an ECU's firmware with vulnerabilities, which an attacker can subsequently exploit.

Attacks against vehicle sensors (34 attacks): include *spoofing* and *jamming* attacks that can be directed towards vehicle GPS, LiDAR or Radar to disrupt vehicle safety and functionality. Other attacks target vehicle cameras, inertial measurement units and environmental manipulation to disrupt the sensors and interfere with the vehicle's operation and systems like anti-lock braking systems.

Attacks against infotainment systems (17 attacks): can serve as a point of entry to affect other vehicle systems, or to steal sensitive data. Attacks include *over-the-air (rogue) updates* and *structured query language (SQL) injection attacks*, which allow an offender to insert malicious queries into applications that use an SQL database.

Attacks against vehicle entry, authorisation and authentication systems (23 attacks): often exploit the keyless entry systems that most vehicles now use and include variations of *relay* and *replay* attacks which involve an attacker intercepting the encrypted signal that vehicle fobs send to vehicles to unlock and start them. Other attacks target vehicle onboard diagnostic (OBD) ports.

Attacks against vehicle data analytics (6 attacks): include those intended to *poison* the data used to train the machine learning systems used by

CAVs, or *adversarial attacks* that use carefully crafted stimuli (e.g. stickers placed on stop signs) encountered in the real-world to trick CAV machine learning systems to misclassify images (e.g. interpreting a stop sign as a 45mph sign) or other inputs collected by the vehicle sensors.

Malware attacks against vehicles (10 attacks): include ransomware attacks, and more generally involve the use of malicious software to disrupt vehicles, gain unauthorised access, or to steal data from them.

Attacks against the vehicle supporting infrastructure (19 attacks): include those against *electric vehicle charging stations*, or those that use the latter to spread malware to CAVs. For example, *toll system attacks* involve intercepting vehicle payment data transmitted via a CAV's short range communication sensors.

## Crime risks for CAVs

In this study, we identified **28 crime threats.** These were rated by an expert group (with representatives from law enforcement, government, industry, and academia) in terms of:

- **Harm -** Victim and/or social harm. Physical or emotional harm associated with an offence, financial loss to an individual, or undermining trust in public institutions would all be considered harmful.
- **Frequency -** The likely number of times the scenario would occur in a period of time.
- **Achievability -** How easy would it be to commit an offense, accounting for likely readiness of the necessary technology and its availability.
- **Defeat-ability -** How easy would it be to develop/apply measures to prevent, detect or render the offence unrewarding (low defeat-ability refers to threats that are difficult to defeat).

To create a ranking of the threats, **an index of risk** was computed by multiplying the harm and frequency ratings together. In this briefing, we describe the top ten high risk crimes and show their ratings for risk and defeatability, before providing brief descriptions of the remaining offences.

| **Top 10 Crime Risks**<br>Rating key: ● Low ●● Medium ●●● High | **Risk** | **Defeat-ability** |
|---|---|---|
| **Illegal transportation -** Using CAVs to remotely transport victims of human trafficking, illegal drugs, weapons, and other illicit goods across locations anywhere in the world. | ●●● | ● |
| **Vehicle part theft -** Targeting vehicles to steal high-value components, such as ECUs and GPS systems. | ●●● | ●● |
| **Vehicle theft (or goods/valuables inside)** - Exploiting weaknesses in keyless entry systems and other authentication technologies to gain unauthorised access to vehicles, either to steal the vehicle or valuables. | ●●● | ●● |
| **Ransom for financial gain** - Cybercriminals may extort money from CAV users by withholding critical vehicle functionalities or data necessary to operate the vehicle. May involve ransomware to disable a CAV by locking it, rendering it unusable, and demanding payment to restore functionality. | ●●● | ●● |
| **Vandalism** - The lack of a driver may make autonomous vehicles more vulnerable to intentional acts of vandalism or damage, such as breaking windows, tire-slashing, and graffiti spray-painting. | ●● | ● |
| **Data theft (to facilitate other crimes) -** Criminals may steal data generated by CAVs, including personal user information or critical vehicle-related details, which could be exploited for other crimes like tracking, manipulation, identity theft, doxing, blackmail, or financial fraud. | ●● | ●●● |
| **Remote control and hacking (computer misuse)** - Exploiting CAV vulnerabilities to gain unauthorised access to CAV systems remotely to facilitate crimes including data theft or unauthorised vehicle control. | ●● | ●●● |
| **Criminal damage -** Causing physical damage to the vehicle itself, other vehicles or property by triggering crashes or malfunctions. | ●● | ●● |
| **Monetary theft -** Exploiting in-vehicle payment services (e.g. for toll payments, fuel purchases, and parking fees) to steal money from vehicle users. | ●● | ●●● |
| **Denying access -** Denying access to a CAV or its features motivated by reasons beyond extortion, e.g. preventing passengers from reaching a destination or using vehicle services. This could be used for indirect monetary gains, to disrupt law enforcement/emergency services, or delay an individual's travel. | ●● | ●● |

## Other Offences (Ranked 11+)

Below, we describe the remaining eighteen crime threats, grouping them by overarching themes.

### Crimes against the person

#### Cyberstalking
The technology used by CAVs such as cameras and sensors (e.g. GPS), could be used to monitor victims or listen to their conversations.

#### Domestic Abuse
The technology used by CAVs, including smart applications and autonomous systems, could be used to (say) restrict a survivor's activity (e.g. where or how far they travel in a vehicle) or gaslight them.

#### Physical Assault
By disrupting CAV safety systems and/or deceiving vehicle sensors, CAVs could be made to cause physical harm (from injuries through to murder) through collisions and other incidents.

### Financial crimes

#### Kidnapping
CAVs could be used to abduct individuals for ransom or other motivations.

#### Insurance Fraud
Offenders may manipulate vehicle data to deceive insurers or potential buyers about vehicle mileage or other things.

#### Cryptojacking
Offenders may gain unauthorised access to CAV computing resources to mine cryptocurrencies.

#### Electricity theft
Offenders may use CAVs to steal electricity from other vehicles or facilities.

#### Leasing fraud
Offenders may tamper with vehicle data (e.g. mileage) to avoid paying fees for leasing violations (e.g. exceeding the permitted mileage).

#### Theft of pay for use features
Many CAVs have pay-for features (e.g. heated seats) that a user may activate without payment.

### Crimes against property or infrastructure

#### Using CAVs to steal (e.g. ram raiding)
CAVs could be used to facilitate ram-raiding without the need for a human driver.

#### Disruption to the National Grid
A fleet of CAVs (e.g. buses or taxis) compromised by a state actor could be made to follow a charging cycle that could affect the national grid, damaging it or forcing it to shut down (as a preventative step).

#### Joyriding
Offenders may gain unauthorised access to CAVs for entertainment, including racing or staging deliberate collisions.

#### Disruption to the food supply chain
CAVs used in the food supply chain could be disrupted, leading to financial losses and food insecurity.

### Terrorist attacks

#### Surveillance for terrorist attacks
CAVs could be used to covertly collect detailed intelligence, including physical security and patterns of patrols, to aid in the planning of terrorist attacks.

#### Terrorism Cyberwarfare
CAVs could be hacked by terrorists to facilitate coordinated attacks, collisions or other attacks.

### Other offences

#### Impersonation
CAVs could masquerade as other vehicles, such as police cars, providing offenders with privileges they could exploit, such as stopping other vehicles.

#### Evasion and obfuscation of criminal liability
Offenders may manipulate the data of vehicles (say) involved in accidents to evade criminal liability.

#### Anti-social behaviour
One or more CAVs could be used to disturb the peace of a neighbourhood by triggering the horns, lights, car alarms or music systems.

## Policy implications

The potential prevalence of CAVs in the future, and the significance of the harm and disruption that could be facilitated by them, requires that action is taken now. This would ideally prevent the threats that might emerge, and address challenges associated with the policing of offences involving CAVs.

#### Challenges for Policing
Future crimes involving CAVs may present novel challenges for law enforcement. For example, the simultaneous unauthorised misuse of many vehicles may create scenarios for which current police resources will be insufficient. Thought will need to be given as to how law enforcement could respond to such incidents, should they occur.

Considering the crime rated as conveying the highest risk in this policy briefing – illegal transportation – approaches to addressing this will likely include the stopping and searching of suspect vehicles. To enable compliance, protocols will be needed to ensure that CAVs can be stopped, when required. Some existing CAVs

(e.g. Waymo self-driving vehicles) have such functionality, and governments (including the UK) are seeking to address this issue. However, methods for detecting illegal transportation and protocols for remotely stopping CAVs are at an early stage and require prioritisation.

### Prevention

CAVs are complex systems that rely on a variety of hardware (e.g. sensors, ECUs), software and machine learning systems. It is critical that these undergo rigorous testing to identify and address vulnerabilities. We advocate for a **secure-by-design** approach such as those that have been widely used in the context of physical spaces, and more recently with the aim of securing the Internet of Things.

The number of components involved in the manufacture of vehicles, and the complicated supply chains that can be required, means that as well as ensuring the security of individual components (where appropriate), attention needs to be given to how those components – designed and produced by different companies – interact. The use of, and compliance with, agreed standards will be important in realising this.

Several regulations, standards and guidelines exist while others are in progress. In particular:

- UN Regulation 155 provides approval requirements and guidelines related to vehicle cybersecurity and cybersecurity management, and UN Regulation 156 covers vehicle software updates.

- Standards include ISO/SAE 21434 which deals with security over the vehicle lifecycle, and ISO 24089 which concerns software updating.

- The ISO/PAS 5112 standard provides guidelines for auditing cybersecurity engineering including secure product development and the maintenance of vehicle software and systems.

- Ongoing international standards include ISO/SAE PAS 8475 which aims to provide cybersecurity assurance levels and ISO/SAE TR 8477 which aims to provide best practices for cybersecurity verification and validation in vehicles.

- The UK Automated Vehicles Act 2024, which regulates the use of automated vehicles. Some of the key features of the Act include an approval and authorisation system, where Automated Vehicles (AVs), including both fully autonomous and those with partial autonomy, must undergo a specific process to obtain authorisation and licensing. AVs must be operated by an authorised self-driving entity to be considered "authorised automated vehicles". To gain authorisation, AVs must meet safety standards that are "equivalent to, or higher than, that of careful and competent human drivers". The Act also introduces the concept of a "no-user-in-charge" journey, where AVs can operate autonomously without a human on board, under the supervision of a licensed no-user-in-charge operator. These licensed operators must meet certain requirements, including having a good reputation, financial standing, and the capability to competently discharge their responsibilities. Overall, the Act provides a general framework for safety standards and authorisation. However, the implementation details of safety and security standards are not addressed by this Act.

Such regulations and standards require significant (and continued) investments from vehicle manufacturers. Moreover, the vehicle industry faces the challenge of implementing security measures that are both effective and scalable, rather than merely superficial efforts designed to meet the minimum compliance requirements. Appropriate assurance mechanisms will also be required to ensure compliance with agreed standards.

The cyber threat landscape is dynamic, with new threats continuing to emerge. Consequently, the assurance mechanisms employed to ensure that vehicles comply with existing standards, and are robust to new attack vectors, must also be dynamic – monitoring compliance at the point of sale will be insufficient. For the vehicles themselves, in the UK, the existing Ministry of Transport (MOT) test[1], an annual test used to check that vehicles meet safety and emissions standards, would provide a mechanism for doing

[1] https://www.gov.uk/guidance/mot-inspection-manual-for-private-passenger-and-light-commercial-vehicles; see also, https://www.gov.uk/government/consultations/changes-to-the-date-of-the-first-mot-test-and-research-into-other-mot-enhancements/changes-to-the-date-of-the-first-mot-test-and-research-into-other-mot-enhancements

this if cybersecurity requirements were introduced. At its most basic, this would require that vehicles have all security updates installed. However, manufacturers will, of course, have to provide such updates, do so in a timely manner and ensure that these meet or exceed agreed standards. The UK Department for Transport is currently considering future changes to the MOT regime that could include CAVs and – given how rapid technological change advances – we strongly encourage that such changes are implemented as soon as possible.

Attention will also need to be given to the infrastructure to which CAVs connect including, but not limited to, the charging network. This adds further complexity and it is important that risk assessments are conducted, and solutions implemented (where necessary), by those who manage the supporting infrastructure associated with connected places[2]. Clarity will also be needed as to who exactly is responsible if different organisations are involved in owning/maintaining the physical infrastructure, managing the charging service, and any other functionality that such networks may offer (e.g. advertising) in the future[3].

What is communicated to consumers at the point of sale is also important. At present, freely available ratings such as Euro NCAP[4] provide consumers with information about vehicle safety, which can inform purchasing decisions, but as far as we are aware, no information is provided about cybersecurity for connected vehicles.

## Methods

- **Four systematic searches** of the academic literature and media reports were conducted to identify cybersecurity issues, and crime threats that might be facilitated by CAVs. More than 150 articles were identified and reviewed, from which a total of 217 cybersecurity threats, and **22 unique crime threats** were identified.
- We subsequently ran a **two-day workshop** with experts comprised of participants from law enforcement, government, vehicle manufacturers, trade associations, CAV technology developers, academia and the voluntary sector. The experts reviewed the 22 crime threats identified in the literature and were then asked to nominate any additional crimes that they could think of. They added **an additional six crime threats**.
- **A rating exercise** was subsequently conducted with participants for which they were asked to rate the crime threats in terms of the harm that they would cause, their likely frequency in the future, how easy it would be to achieve them (by offenders) and how difficult it would be to address them (e.g. by governments, law enforcement, or industry).

## Funders

This research was funded by the Dawes Centre for Future Crime at UCL. **The Dawes Centre for Future Crime at UCL was established to identify how technological, social or environmental change might create new opportunities for crime and to conduct research to address them.**

The Dawes Centre is funded by the Dawes Trust and UCL. These funds are limited and so we invite additional funding from the public and private sector. By funding the Centre you will contribute to helping society better prepare for crimes of the future. We are also able to undertake research upon request, contributing to organisational goals and strategic thinking.

## Find out more about the research

A full academic paper that describes what CAVs are, the cybersecurity threats they are vulnerable to and the crime threats they might facilitate is available at:

https://doi.org/10.1186/s40163-025-00245-x

## The authors

Dr Nilufer Tuptuk, UCL
Mr Ashley Brown, UCL
Professor Shane D Johnson MBE, UCL

**Contact:** Mr Vaseem Khan, Strategic Alliance Director, UCL Security and Crime Science **vaseem.khan@ucl.ac.uk,** or Professor Shane Johnson, Director, Dawes Centre of Future Crime at UCL, **shane.johnson@ucl.ac.uk**.

[2] https://www.gov.uk/guidance/secure-connected-places;
[3] https://www.ucl.ac.uk/steapp/sites/steapp/files/policy_brief_strengthening_cyber-resilience_and_procurement_frameworks_for_connected_places_-_final_version_0.pdf
[4] https://www.euroncap.com/en/