Journal of Transportation Security
https://doi.org/10.1007/s12198-021-00236-4

Risk analysis for forecasting cyberattacks against connected and autonomous vehicles

Sunniva F. Meyer[1] · **Rune Elvik**[1] · **Espen Johnsson**[1]

Received: 29 September 2020 / Accepted: 13 September 2021

Abstract

A security risk analysis was conducted to identify possible cyberattacks against a future transport system consisting of autonomous and connected vehicles. Six scenarios were developed: joyriding, kidnapping, domestic abuse, autopilot manipulation, a large transport accident, and paralysis of the transport system. Even if it were possible to increase the difficulty of conducting such cyberattacks, it might be impossible to eliminate such attacks entirely. Measures that limit the consequences will therefore be necessary. Such measures include safety measures in vehicles to protect their occupants in traffic accidents and measures that make vehicles easier to remove in case they do not function.

Keywords Cybersecurity · Forecasting crime · Vehicle crime · Standardization · Risk analysis

Introduction

The proliferation of connected and autonomous vehicles provides new opportunities for crime, whether such vehicles constitute a target, a container for human targets or other valuables, or a tool for committing other crimes. Predicting crime is one of the enduring challenges for the security community (Virta 2019). Connected and autonomous vehicles present a particular challenge for society, because it will be possible for remote attackers to hack into them, or for such vehicles to be used driverless to commit crimes, in effect anonymizing the offender (Newton 2016).

Technological change has always influenced opportunities for crime. Transportation technology reduces the time and cost of travel (Newton 2016). Thus, not only law-abiding citizens benefit from saving time and money when traveling. Criminals benefit, too, by being able to move about more easily and inexpensively (Newton 2016). Cyberspace transcends the usual spatial limits by widening the range of offenders and

✉ Sunniva F. Meyer
sfm@toi.no

[1] Institute of Transport Economics, Oslo, Norway

Published online: 12 November 2021

victims and by increasing the possible convergences between them (Felson and Eckert 2018). Cyberspace also offers new crime forms, such as seizing control of computers to serve one's own purposes (Felson and Eckert 2018). Through bad design, technology can render vehicles vulnerable, attractive, or provocative to offenders. Through good design, it can render vehicles resistant, unattractive, and unprovocative (Ekblom 2017). Evidence suggests that there is a lag between the emergence of new crimes and awareness of and preparedness for them (Furnell 2017).

Originally, vehicles were mechanical only, but in recent vehicles, more and more of the mechanical parts have been augmented or replaced by small computers, so-called electronic control units (ECUs). ECUs can support various wireless network protocols, such as Wi-Fi, Bluetooth, and vehicle-to-everything (V2X) communication, where V2X is the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. In 2018, the average vehicle had 25 ECUs, while some high-end models already had over 100 ECUs (Claburn 2018). Many of these ECUs in recent vehicles have been poorly protected because they have been designed to prioritize simplicity (Claburn 2018). Such ECUs make vehicles vulnerable to cyberattacks and research has shown that it is possible to conduct cyberattacks, such as draining the battery, even when the engine is not running (Cho et al. 2018).

The number of ECUs is only increasing in modern vehicles, and autonomous vehicles will probably eventually be characterized as "data centers on wheels" (Thomson 2018). The increasing number of sensors and other ECUs with wireless network protocols will increase the number of possible entry points for potential hackers and thus increase the salience of cybersecurity.

Von Solms and van Niekerk (2013) define cybersecurity as "the protection of cyberspace itself, the electronic information, the information and communications technologies that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace." Accordingly, cybersecurity for transport systems consisting of autonomous and connected vehicles includes protection of software, such as programs enabling V2X communication; hardware, such as vehicles and servers; the users of the transport system, and the data about users and the transport system.

Our purpose in this paper is to forecast the effects of the proliferation of connected and autonomous vehicles on the cybersecurity of the transport system. Such knowledge could both inform government policy for autonomous vehicles and provide input for industry to assess and mitigate risks related to cybersecurity. We will forecast such effects on cybersecurity by conducting a risk analysis as described by the Norwegian Standard for Security Risk Assessment (NS 5832:2014).

Method

Standards Norway is a private and independent member organization, and is one of three standardization bodies in Norway. Standards Norway is responsible for standardization activities in all areas except the electrotechnical field and the telecommunications

field (Standard Norge 2021). Standardization is based on the basic principles of openness, independence, voluntariness, and consensus. Participation in the standardization work is voluntary, and all interested parties are invited to be represented (Standard Norge 2013).

Standards Norway appointed the national committee SN/K 296 "Societal Security in Construction, Civil Engineering and Real Estate" in 2010 (Sektorstyret BAE 2010). SN/K 296 has the mandate to prepare documents in the form of standards, guidelines, etc. which concern societal security in the built environment (Sektorstyret BAE 2010). The committee is responsible for developing the 5830 series, which builds on ISO 31000 "Risk management – Guidelines," but goes more in depth on some elements (especially in NS 5832).

The Norwegian Standard for Security Risk Assessment (NS 5832:2014) describes how to carry out a risk analysis when the probability is difficult or impossible to calculate (for example because historical data are lacking). Excluding probability, however, entails that the focus is shifted from what is probable to what is possible, and the shift could result in too great a focus on worst-case scenarios (Jore 2019). Because autonomous and connected vehicles have not yet been widely rolled out, it is not meaningful to calculate probabilities for different incidents. NS 5832:2014 is therefore deemed to be a suitable standard to follow when conducting a risk analysis.

The security risk assessment, as described in NS 5832:2014, has seven steps:

(1) Consequences assessment
(2) Determination of security objectives
(3) Threat assessment
(4) Scenario selection
(5) Vulnerability assessment
(6) Assessment of pure (negative) risk
(7) Presentation of the risk situation.

Consequences assessment (1) consists of mapping, assessing, and ranking the assets (both material and non-material). Determination of security objectives (2) involves deciding what are the desired or acceptable conditions for the assets during or after an undesired event. The threat assessment (3) should identify and describe possible malicious actors, their intention(s), and their capacity for attacking. Scenario selection (4) should result in scenarios that are based on assessments of consequences and threats, and is considered as relevant for further analysis. The vulnerability assessment (5) should describe which assets are vulnerable in the selected scenarios. Finally, the assessment of pure risk (6) should compile the results from the consequences, threat, and vulnerability assessments to produce an assessment of the pure risk for each scenario, and the presentation of the risk situation (7) should summarize the pure risk for all selected scenarios.

Risk analysis

Consequences assessment

A traditional transport system consists of the following:

(1) vehicles (cars, buses, bicycles, etc.)
(2) the infrastructure the vehicles use (roads, bridges, tunnels, the network of fuel providers, etc.)
(3) transport providers (taxi drivers, public transport companies, logistic companies)
(4) people using the transport system, including passengers in vehicles, bicyclists, pedestrians, and children that play in the streets
(5) commodities being transported

A transport system with connected and autonomous vehicles will also include connectivity elements:

(6) systems collecting, processing, and distributing information about weather, traffic, and road work to enable vehicles to optimize travel choices
(7) platforms for ordering and distributing vehicles wherever and whenever transport is sought
(8) servers providing (automatic) updates of vehicles

Finally, the transport system will collect vast amounts of data:

(9) data about when and where people travel.

Which of the above elements are critical for the functioning of the transport system? (1) No single vehicle is critical for the transport system as such, but connectivity makes it possible to immobilize a large share of the vehicles, which can seriously hinder transport. (2) The infrastructure the vehicles use is the same as is used by non-autonomous vehicles. Some parts of the infrastructure can be bottlenecks (bridges, tunnels, etc.) and these points could be clogged by immobilized vehicles or by the hacking of equipment (barriers, traffic lights, etc.) installed at such points. (3) Most transport providers are not critical for the transport system. An exception might be monopolists in an area. (4) A single person is not critical for the functioning of the transport system. Public incidents where individuals are killed, seriously hurt, or hijacked in an autonomous vehicle might, however, scare the general public about using autonomous vehicles. (5) Most commodities are not critical for the functioning of the transport system.

(6) Systems that provide information for vehicles to optimize travel choices increase the efficiency of the transport system, but are not critical for its functioning. Downtime or misinformation in such systems, especially if there exists only one such system, can create traffic jams. (7) Platforms for ordering and distributing vehicles are critical in a situation where all vehicles are for public hire, instead

of private. In a situation with few platforms for ordering and distributing vehicles, these platforms can be critical for the functioning of the transport system. (8) Servers providing (automatic) updates can compromise a large number of vehicles simultaneously so that so many are not working, that is, clogging the streets, that the transport system stops working properly.

(9) The data produced are also part of the transport system. Data about individuals' travel patterns are sensitive. Such data can provide sensitive information about individuals, and if such data are compromised, trust in the transport system could be reduced. Data about travel patterns at a higher level will be used to plan the transport system and could be misused by malicious actors.

A final value connected to (4) and (9) is confidence in the transport system. If potential users do not believe that it is safe to use the transport system, they might choose to not use it. Fear of being killed, being hurt, or being the victim of crime might make people not travel.

The most important value is of course the people using the transport system at any given time. However, the likelihood of managing to kill all users of a specific transport system in one cyberattack is low. Cyberattacks causing a few deaths do not per se threaten the transport system. Individual elements that can be critical for the functioning of the transport system are the following:

(1) servers that provide updates to a large number of vehicles
(2) platforms ordering and distributing transport
(3) physical bottle necks in the transport system
(4) energy refilling infrastructure.

In addition, when people have the option of not traveling or of using alternative transport, (5) confidence in the transport system also is a critical value for the transport system.

Security objectives

Before delving into incident-specific security objectives, we discuss some general security objectives for connected and autonomous vehicles.

1. There should be an absolute reduction in the number of deaths and seriously injured compared to current deaths and injuries, and a reduction in the risk of being killed or seriously injured per kilometer traveled. This objective is not especially ambitious given that some countries already aim for zero fatalities and serious injuries from traffic accidents.
2. Cyberattacks should not impose larger costs on society than the benefits of efficiency gains achieved by introducing connected and autonomous vehicles.
3. Breakdown time should be a maximum of 48 h per year. Heavy snowfall causes schools, public transport, and other public functions to close down many places and at least 48 h of downtime per year is not uncommon.

4. Breakdowns in the transport system should not cause so many delays in emergency responses that the number of people dying and the economic costs exceed the gains of the first and second objectives.
5. Confidence in the transport system should be so high that 95% of the population are willing to travel by connected and autonomous vehicles.
6. Confidence in the transport system should be so high that 90% of the population report that they feel secure when traveling in connected and autonomous vehicles.

The general security objectives can be translated into incident-specific security objectives that is, the desired or acceptable conditions for the assets during or after an undesired event. A difficult question is whether it matters how large the consequences of a single cyberattack are when the consequences of all cyberattacks do not exceed those acceptable per the general objectives (as described above). For the objectives of number of deaths and seriously injured and economic costs of cyberattacks, it normatively does not matter whether the unwanted consequences are caused by one large incident or several smaller incidents. Large incidents might cause more attention and thus fear, but for society it may be irrelevant whether all the deaths and injuries happen in a particular month or are distributed throughout the year. For downtime of the transport system, the answer is different: Short delays seldom have large consequences, while longer delays can cause shortages of commodities, etc. The general objective of confidence in the transport system might be achievable most of the time, but perhaps not just after a cyberattack that has caused significant damage and/or received significant attention.

1. No cyberattack should cause more deaths and serious injuries per year than defined by the first general security objective.
2. No cyberattack should cause larger economic costs per year than defined by the second general security objective.
3. No cyberattack should cause more than 24 h of downtime of the transport system.
4. No cyberattack should delay emergency responses such that people die, fires develop further, and conflict situations escalate into violence because of the delay.
5. Seven days after a cyberattack, at least 90% of the population should be willing to resume using autonomous vehicles.
6. Twenty-one days after a cyberattack, at least 80% of the population should report that they feel safe as passengers of autonomous vehicles.

Threat assessment

"Hacking" refers to "activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks" (Malwarebytes 2019). Connected and autonomous vehicles are examples of digital devices that can be hacked.

Hackers can be divided into categories according to their motives and skill levels. Individuals who wish to manipulate computer systems, but lack the ability to manipulate computer technology at high enough levels, are considered "low-tech attackers" (Graham and Smith 2019). "Script kiddies," for example, have generally no or

few programming skills. They may therefore search the internet looking for hacker utility programs and then launch the programs against a target. Such programs are already available for conducting attacks against connected and autonomous vehicles (Sanguino et al. 2020). Script kiddies can be especially dangerous because they seldom understand how the program will affect the target system (Moore 2014). But hackers can also use psychology to trick the user into clicking on a malicious attachment or providing personal data. These tactics are referred to as "social engineering" (Malwarebytes 2019). Furthermore, control systems in autonomous vehicles suffer from limitations that can be exploited by a malicious attacker. For example, the autopilot of Tesla vehicles has been shown to interpret white crossing vehicles as brightly lit sky and to act accordingly (Hawkins 2019). A malicious attacker could change the physical environment to make the control system in the autonomous vehicle act differently. In this analysis, we will use the term "autopilot manipulation" to describe malicious attacks where the attacker changes the physical environment to manipulate the autonomous vehicle to act differently.

The literature distinguishes between three main types of high-tech hackers (Graham and Smith 2019; Moore 2014): black-hat hackers, white-hat hackers, and grey-hat hackers. Black-hat hackers violate computer security for maliciousness or for personal gain. White-hat hackers are the opposite of black-hat hackers. They still search out targets and attempt to hack into systems, but they do so to provide security programs that will protect systems from being illegally and maliciously penetrated. Grey-hat hackers are a combination of white- and black-hat hackers. If a gray-hat hacker searches the internet for a target and successfully gains access to a computer system, he or she might notify the system owner and, instead of telling the administrator how the system was exploited, offer to repair the defect for a small amount of money.

It is also possible to distinguish hacker types by other features, such as capacity: The lone hacker (i), an ad hoc group (ii), an organized group (iii), a state-supported group (iv), and a state (v).

(i) A lone attacker may have varying degrees of programming skills, but commits the attack alone, which often limits what the attacker can do. An example of a lone attacker would be a rejected lover wanting to take revenge by stealing information from the ex-lover's digital device and then using it to destroy that person's life.
(ii) An ad hoc group is a temporary group formed of people with hacking capabilities to do some mischief. They do not have a formal hierarchy, but have a common goal, such as sabotage against an organization, a company, or the authorities, or financial gain.
(iii) An organized group collaborate frequently and have designated roles, which enables the group to employ its human resources more efficiently in a cyberattack.
(iv) A state-supported group is an organized group supported by a government and thus has even more resources available when attacking. Such groups typically inflict harm that the government wants to inflict but cannot be publicly seen to inflict.

(v) We say that the attack is conducted by the state if any part of the governments' formal organization conducts the attack.

Cybercriminals can also be distinguished by motive. Zamora (2018) lists six main motives for hacking: for fun/the challenge (a), financial (b), emotional (c), ego (d), political/religious (e), and sexual impulses/deviant behavior (f).

(a) Fun/the challenge: When the Black Report (Pogue 2018) asked hackers about why they hack (several answers were possible), 86% replied that they liked the challenge of hacking and hacked to learn. Additionally, 35% said they hacked for the entertainment value or to make mischief (Pogue 2018).
(b) Financial gain: In the Black Report's survey, 21% of respondents replied that they hacked for financial gain (Pogue 2018).
(c) Emotional: Some of the most destructive cybercriminals act out of emotions, such as rage, revenge, or despair. These criminals may cyberstalk, access accounts without authorization, or use the Internet of Things (IoT) to commit domestic abuse (Boyd 2018; Zamora 2018).
(d) Ego: Strengthening a weak ego is a motivation that can be caused by several psychological vulnerabilities, such as insecurity, financial woes, and emotional turmoil (Zamora 2018).
(e) Political/religious: Six percent of the hackers in the above survey replied that they hacked for social or political motives. Such activities can be labeled as hacktivism, cyberterrorism, and/or state-supported cybercrime (Zamora 2018).
(f) Sexual impulses/deviant behavior: The sixth and last category is a group in the darkest corners of the web to whom sexual compulsion and deviant behavior apply. Rapists, sexual sadists, pedophiles, and even serial killers use their own skill or hire those lacking a moral compass to aid them in their sexual predatory behaviors (Zamora 2018).

Scenario selection and vulnerability assessment

We have created six scenarios for further analysis. These scenarios cover 4 of 6 motivations for hacking (for fun/the challenge, financial, emotional, political/religious) and 5 of 5 actor capacities (lone actor, ad hoc group, organized group, state-supported group, state).

Joyriding

Three teenagers want to remotely control a full-sized vehicle. One has an uncle who has just bought a fully autonomous vehicle and they decide to hack it to use as a remote-controlled vehicle. They have access to the uncle's home where they find the vehicle's ID and other information about the vehicle that makes it easier to hack.

When he is on holiday, they hack the vehicle and manage to get it to travel from the uncle's home to their school. They discover, however, that they cannot control the vehicle's speed. They search the internet for software that makes it

possible to control the speed. They find such software and manage to install it on the vehicle's computer.

They make the vehicle drive into the street again and this time faster than the speed limit and faster than the road environment permits. The vehicle drives past a lawn where children are playing with a ball. The ball ends up in the street and a child runs after it. The autonomous vehicle's sensors detect the child, but the vehicle's speed is so high that it cannot slow down enough before it hits the child, and the child is killed immediately.

In this scenario, two assets are damaged: the child and the vehicle. The vehicle can probably be repaired, but the child is dead. Another possible consequence is that people start to fear autonomous vehicles and therefore do not let their children go out and play. Such limitations on children's physical activity can have detrimental effects on public health.

Kidnapping

A group of organized criminals, looking for new ways to make money, recruit hackers and decide to kidnap the ten-year-old child of a billionaire living nearby, who has just bought one of the newest autonomous vehicles available. The hackers suspect it has been released on the market prematurely and that it has software bugs that can be exploited in a cyberattack.

The hackers successfully gain access to the in-vehicle system and manage to install surveillance software. They are able to follow the vehicle's movements in real time and to listen to communications and other sounds inside the vehicle. They quickly discover that the child attends dancing lessons every Tuesday evening. They also gain access to the control system and locking system.

They decide to strike one such Tuesday evening. When the child is on the way home, they lock the vehicle and make it impossible for the child to open it. They also hijack the vehicle, driving it to a predefined site in a forest. When the vehicle arrives, they open the locks and move the child to a prepared hiding place where they make a ransom movie that shows the child is physically ok and in which they present their ransom demand. When they have received the money, they return the child to the parents.

Initially, the parents do not publicize that they paid a ransom, and keep the hijacking secret. However, after deliberating with their lawyers, they decide to sue the manufacturers of the autonomous vehicle for not having invested enough in cybersecurity to prevent such hijackings.

In the kidnapping scenario, only the ten-year-old child is under physical threat. However, both the child and the parents experience trauma, which might reduce their quality of life for years. After the public is made aware about the kidnapping, people who perceive themselves as attractive targets for such crimes start avoiding autonomous vehicles and instead choose to travel by older, non-autonomous vehicles.

Domestic abuse

An IT expert has been rejected by a lover after they dated some months. The ex-lover had just obtained an autonomous vehicle and all the user information and documentation was lying around in the ex-lover's apartment, easily accessible for the IT expert. The IT expert was curious about the technology and had therefore read all the documentation when visiting the ex-lover.

The break-up is ugly and the IT expert feels hurt and badly treated by the ex-lover. The IT expert decides to take revenge by playing some tricks on the ex-lover. The IT expert succeeds in hacking the vehicle, accessing the control system, the air conditioning/heating system, and the locking system.

The IT expert conducts the cyberattack one cold winter morning when the ex-lover is traveling to work. First, the IT expert locks the doors and makes it impossible for the ex-lover to open them. Then the IT expert makes the vehicle drive a new route where it can drive at least 70 km per hour for many hours. Finally, the IT expert turns off the heating system, which makes the temperature in the vehicle very low, and turns on the sound system, making it loudly play music the ex-lover dislikes.

The ex-lover quickly discovers that something is very wrong with the vehicle and calls an emergency number. The police try to find the vehicle, but experience some difficulty with intercepting it because the route is confusing and they therefore do not know where it is traveling next. Finally, after approximately an hour, they manage to intercept it and force it to stop.

The ex-lover is physically unhurt, but very traumatized. News coverage of the incident reduces people's confidence in autonomous vehicles, resulting in less use of autonomous vehicles, and perhaps more use of manual vehicles, which will tend to be older and less environmentally friendly.

Autopilot manipulation

The introduction of autonomous vehicles has made private vehicle transport much more attractive and has thus caused increased traffic. Even if the new vehicles cause fewer or no exhaust emissions, they create particulate matter because of wear and tear when their tires meet the road surface. The increased traffic has therefore caused increased local pollution and reduced air quality.

Environmental organizations are furious about what they perceive as politicians' lack of willingness to cope with this increased traffic, and one of the more radical organizations decides to act. They want to reduce confidence in the transport system by exposing vulnerabilities of the autopilots and thereby decrease the use of autonomous vehicles.

Many local branches decide to launch a coordinated campaign. They decide on a date and time for demonstrations. They create physical dummies to mislead the autopilot into believing that the lane is going straight ahead whereas it is actually turning (left or right) instead.

Most branches succeed with misleading the vehicles to run off the road. They are seriously damaged, while passengers suffer mostly minor injuries and trauma.

One branch, consisting of really furious teenagers, decides to mislead the vehicles to drive into the lane with oncoming traffic, causing one large traffic accident that seriously injures several people.

In this scenario, many people sustain minor injuries and a few sustain serious injuries. Many vehicles are damaged. The incident also causes reduced confidence in autonomous vehicles, resulting in less use of the transport system and more use of older and less environmentally friendly vehicles.

Large transport accident

Two neighboring countries have an ongoing border conflict and repeated negotiations have not solved it. A discovery of valuable natural resources in the disputed territory has increased the salience of the conflict and one country wants to flex its power.

Since the countries are not officially at war, the authorities want to avoid being directly involved in the attack. They have, however, for some time been supporting organized hacker groups. They ask one of these state-sponsored groups to create some random and very visible damage in the transport system of the other country. They want it to be possible to discover the country where the cyberattack originated, but it should not be possible to attribute the attack to them.

The state-sponsored group has the capacity to conduct several parallel attacks. Beforehand, they explore known security flaws in vehicles' sensors. They create several scripts that together can compromise so many sensors that the vehicles will be confused. The scripts conduct so-called slight attacks, attacks that are so small they are not discovered by the vehicles' security systems (Li et al. 2018). In addition, they create scripts that enable them to adjust the vehicles' headlights. Finally, they hack a server that is monitoring traffic in real time to obtain information about which vehicles are near relevant sites at any time.

The state-sponsored group choose to attack in the winter, when it is dark in the early morning and roads are slippery. They choose an area centered on a fast-paced roundabout where they know there will be some snow and/or ice despite many vehicles traveling through it. They attack several sensors on all vehicles in the area. In addition, they increase the intensity of vehicles' headlights so that drivers of other vehicles are blinded. The security systems on some vehicles detects the attack and is able to counter it, but a sufficient number of vehicles are still successfully hacked. The cyberattack results in a large traffic accident involving 10 vehicles and causing several fatalities and seriously injured people.

Investigation of the traffic accident reveals it was caused by a sophisticated cyberattack.

In this scenario, many people are seriously injured and some are killed. Many vehicles are so damaged that they are scrapped. It takes many hours to clean up after the incident, resulting in long queues and reduced accessibility in the area. Public confidence in autonomous vehicles is significantly reduced and many people stop using them for a while.

Paralysis of the transport system

Two countries are currently on the brink of war and one of them has decided to openly demonstrate its cyber capabilities.

Through public sources, its intelligence services find out the respective shares of different vehicle brands in the target country's vehicle inventory. They select a vehicle brand with a 23% share of the inventory. Then they identify the server that the vehicles receive over-the-air updates from. They eventually gain access to the server without being discovered.

Next, they add a hostile program to a scheduled update. The program is supposed to make all vehicles stop wherever they are located at 4 p.m. on a specific date (a weekday) after the scheduled update. The program successfully infects all targeted vehicles without being discovered.

On the chosen date, the hostile program switches on and all targeted vehicles stop abruptly. Many trailing vehicles do not manage to stop on time, resulting in multiple traffic accidents countrywide. The immobile vehicles block other traffic, making it impossible to travel by vehicle in many densely trafficked city areas. The immobile vehicles also impede emergency vehicles, delaying emergency responses and making it impossible for emergency vehicles to gain access to some inner-city areas.

The sudden paralysis of the transport system causes many minor traffic accidents with resulting vehicle damage and personal injuries. The consequences of the continued blocking of traffic are more serious. Trade flows are disrupted, causing damage to property and non-delivery of time-critical goods. Emergency vehicles are either delayed or unable to arrive at all, causing fires to develop further and people to not be rescued in time.

Summary

In most of the above scenarios, only a few people are afflicted directly. Only the last two scenarios affect more than a few people. All scenarios can, however, if made public, threaten public confidence in the transport system, and thus make people rather travel by older manual vehicles which have less crash protection and are less environmentally friendly.

Pure risk

For each scenario, we ask:

1. Is it plausible that there are people who are motivated to conduct such cyberattacks?
2. Is it plausible that anyone motivated to conduct such cyberattacks also has the ability to implement them?

3. Is it plausible that vehicle developers will not invest enough resources in cybersecurity to prevent such cyberattacks either

   (i) because they lack incentives to spend the necessary resources on cybersecurity?
   (ii) because it is impossible to totally secure against a high-capacity attacker?
   (iii) or because of both the above?

Question 3 is included because fully autonomous vehicles are being developed, and developers still have the opportunity to design built-in security, such as building encryption and cryptographic code for signing into a vehicle's systems, minimizing the attack surface hackers can exploit, and tightly locking down communications with the outside world (Thomson 2018).

Many autonomous vehicles already on the roads are connected and thus vulnerable to hacking. The industry has until now been unwilling to invest the necessary resources in cybersecurity to prevent hacking. Developers design components based on old hardware and software with basic inherent flaws, so errors and vulnerabilities are transferred to new generations of vehicles (Sanguino et al. 2020). One possible explanation is that vehicle manufacturers have failed to realize that secure software is critical for automotive safety (Consumer Watchdog 2019). This explanation was more plausible a few years ago before several well-publicized hacking demonstrations (Osborne 2018).

Another possible explanation is that the industry is in a state of Nash equilibrium whereby all major vehicle manufacturers are aware of the risk of hacking, but no one is motivated to unilaterally increase expenditures on cybersecurity. Investing in cybersecurity diverts resources from the development of customer-visible features and thus makes those manufacturers who invested in cybersecurity less competitive. Since hardware and software differ between manufacturers, an actual cyberattack will probably hit only one manufacturer. Each manufacturer may therefore prefer to gamble on not being targeted in a cyberattack until external forces, such as regulation, force them to increase expenditure on cybersecurity (Consumer Watchdog 2019).

A third possible explanation for limited cybersecurity is that manufacturers want to be able to harvest data to monetize them. To ensure that it is possible to harvest data, all vehicle data must be downloadable and thus is vulnerable to malicious access.

Joyriding

Remotely controlled toys are popular, and it seems plausible that some people would want to use autonomous vehicles as remotely controlled toys to play with. It is even more plausible that people without rightful access to a vehicle will be motivated to try to gain access to others' vehicles, since vehicle thefts for joyriding are already common.

In the past, cloning electronic keys has been the most common way of gaining unauthorized access to a vehicle. But vehicles are becoming more connected via technologies such as Wi-Fi and 3G, 4G, and 5G, giving hackers multiple ways to gain access. More than a quarter of current attacks exploit vehicles' cloud servers or mobile apps (Bird 2019). In Britain, vehicle thefts have increased by 50% in five years partly because of criminals hacking keyless systems (Hull 2019). In this scenario, teenagers even have access to the vehicle owner's home, which may make it even easier to gain control over the vehicle.

Vehicle manufacturers will have to deal with the risk of vehicle theft. GPS and other types of tracking might reduce thefts motivated by financial gain, but will not have the same preventive effect against perpetrators who want only to "borrow" the vehicle for a limited time. And even if manufacturers spend enough on protection against access by strangers, it still might be possible to take control of a vehicle if one has access to the vehicle owner's home. Hence, it seems probable that scenarios where people illegally play with other people's autonomous vehicles will occur.

Tampering with an engine's speed governor to make a vehicle able to drive faster is also quite common, partly because doing so rarely leads to penalties for the vehicle owner or other people responsible. And if anyone can create software that makes the vehicle drive faster than it is programmed to, they may also make the software available for anyone on the internet. Will manufacturers spend enough on cybersecurity to counter such hacking attempts? Because so many people might be motivated to manipulate autonomous vehicles' speed, there is a significant probability that a few of them will discover and exploit any vulnerabilities in the programming. It might therefore be impossible to stop such hacking from happening at all. But it might be possible to monitor what hacking software is available and send updates that counter such software whenever manufacturers discover its existence. It can also be possible to monitor vehicles' speeds in real time to detect whether the speed controller has been manipulated.

A related question is whether manufacturers will have incentives to spend the necessary resources to prevent speed manipulation. That depends on whether they are held responsible for accidents caused by speeding due to hacking of speed controllers. If manufacturers can claim they have no responsibility for a traffic accident because someone modified the vehicle's programming, they may not be willing to spend the necessary resources to prevent hacking of speed controllers. But if they are held responsible for not preventing such hacking, they will probably be willing to do whatever is required to limit its extent.

In summary, if manufacturers spend enough resources to prevent manipulation of vehicles' speeds, the worst consequences can be prevented.

Kidnapping for ransom

Many people may be motivated to obtain private data about mobility patterns, including criminals planning to commit crimes against persons or property. If it is possible and they have the capacity, they will try to obtain such private data when they prepare for such crimes. Two important questions: Will developers choose to

protect against such unlawful access to private data? And will manufacturers be held responsible if such data are unlawfully obtained?

For manufacturers to be held responsible, it must be discovered that private data about mobility have been unlawfully accessed. In many situations, detection can be difficult. And even if such data are used to conduct a crime against persons or property, it might still be a problem proving that the crime in question was made possible by unlawful access to private data. It is therefore uncertain whether manufacturers will be willing to spend the necessary resources on protecting vehicle users' private data.

In the kidnapping scenario, kidnappers gain access to the vehicle's control and locking systems. The control system is vulnerable because it is remote-controlled. Expert hackers could plausibly spoof the real owner's signals. The locking system is also vulnerable because modern vehicles are keyless, making it easier for malicious actors to open and lock them.

In summary, it seems plausible that organized criminals can exploit new vulnerabilities of autonomous vehicles and more easily organize kidnappings without being caught.

Domestic abuse

Using modern technology when conducting domestic abuse is not a new phenomenon; for years, a subset of abusive partners with technical knowledge have placed spyware on computers or mobile devices, stolen passwords, and generally kept tabs on their partners (Boyd 2018). Hence, it is highly plausible that domestic abusers having the necessary technical capability may choose to use autonomous vehicles as a tool for terrorizing their victims.

In the domestic abuse scenario, the IT expert unlawfully gains access to the control and locking systems. In addition, the IT expert gains control over the air conditioning/heating system and the sound system for the purpose of increasing the exlover's discomfort during the drive.

The researchers Charlie Miller and Chris Valasek demonstrated already in 2015 that they could hack a Jeep Cherokee and control both its air conditioning/heating system and its sound system (Osborne 2018). Because of the convenience of entering a vehicle that has a comfortable temperature, the air conditioning/heating system will probably also be remotely controlled, and thus vulnerable to hacking. A relevant question is whether developers will prioritize protecting the air conditioning/heating system and/or sound system from hacking. Since hacking such systems would primarily make traveling less comfortable, and the consequences of such discomfort are unlikely to be severe, developers might think that less security would be needed. There might, however, exist manual solutions for protecting against cyberattacks against air conditioning/heating and sound systems, such as including a manual switch that disconnects the air conditioning/heating and sound systems from all networks.

In summary, domestic abuse is very common, but only a very few domestic abusers have the technical knowledge needed for hacking an autonomous vehicle. Access to the victim's home may, however, help a would-be hacker to obtain the necessary

knowledge for conducting a cyberattack. Hence, as well as investing in security to protect the control, locking, and air conditioning/heating systems, measures that support vehicle owners in protecting "inside information" about their vehicles might reduce cyberattacks relying on such inside information.

Autopilot manipulation

Environmental groups engage in a mixture of political methods and activities, everything from confrontation and violence to more conventional styles of political persuasion (Dalton et al. 2003). In many cases where more conventional styles of political persuasion fail, such groups may choose to conduct protests of a more irregular nature. Hence, some environmental groups could plausibly conduct a campaign such as the one described above.

Artificial intelligence is vulnerable and early versions of autopilots have demonstrated some of the vulnerabilities. The autopilot of Tesla models has misinterpreted the broad side of large white semi-trailers as the bright sky, leading to two fatal traffic accidents, the first in 2016 and the second in 2019 (Hawkins 2019). Since the problem with misinterpretation was not fixed despite the first fatal accident and indeed still exists *to this day*, the problem is clearly difficult to solve. It is also reasonable to assume that more vulnerabilities will be discovered when autopilots/autonomous vehicles become more common. Such vulnerabilities can be exploited in protests.

Some researchers have actually succeeded in tricking a Tesla's autopilot into driving into oncoming traffic. They used a can of paint and a brush to mislead the Tesla into the oncoming lane (Tencent Keen Security Lab 2019). Developers are undoubtedly doing their best to improve autopilot software and eliminate vulnerabilities. It is, however, uncertain whether they will be able to eliminate all such vulnerabilities.

In summary, political organizations sometimes choose to conduct irregular protests. For example, some of these organizations might choose to change the physical environment to manipulate the autopilots of autonomous vehicles. Such an attack will require only limited technical knowledge. It is uncertain whether vehicle developers could create autopilots without vulnerabilities that could be exploited in such an attack.

Large transport accident

Neighboring countries must interact regularly because of cross-border issues. Such interaction will sometimes lead to disputes, either public or private. If one of the countries is seriously provoked, it may want to secretly damage the neighboring country without being held publicly responsible. A covert operation is "an operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor" (Office of the Chairman of the Joint Chiefs of Staff 2019). State sponsorship of hacking groups is a relatively easy way to conceal the identity of the sponsor and is a serious challenge for holding states accountable and for ensuring that retaliation is directed at the right place (Doffman 2019).

Currently, autonomous vehicles are using only one or two sensors for object detection, which makes them vulnerable for spoofing attacks (Campbell 2018). Spoofing GPS signals, for example, could send the vehicle the wrong way on a one-way road (Goodin 2018). The inherent interconnectivity between multiple sensors and communication layers of autonomous vehicles offers more entry points and could, in theory, make such vehicles more exposed to cyberattacks. However, finding access to a multilayered system that integrates information coming from several sensors is also more difficult (Buttice 2019; Soare 2019). If hackers manage to spoof one sensor, the main computer might notice discrepancies between data from the spoofed sensor and other sensors, and implement security procedures. To avoid detection, an attacker may therefore need to attack several sensors in a coordinated attack, which is much more demanding. Accordingly, a successful attack requires a coordinated attack on several sensors. Only high-capacity attackers can conduct such an attack.

Unlike the locking and control systems, vehicles' headlights do not need to be remotely controlled. It should therefore be easier to protect vehicles' headlights from cyberattacks. An important question is, however, whether developers will invest enough in protecting vehicles' headlights from cyberattacks. Developers might assume that few hackers would be motivated to attack vehicles' headlights and that the consequences of such an attack would be minor. It is therefore uncertain whether developers would be willing to spend the necessary resources to protect vehicles' headlights from malicious cyberattacks.

There will probably be many different servers that monitor traffic. Some may be provided by hi-tech companies with extensive resources and others may be provided by smaller actors that may not have the resources or skills to protect servers from hacking. Even in cases where companies are willing to spend extensive resources on cybersecurity, servers will be vulnerable to hacking from high-capacity attackers. Even hi-tech companies, such as Apple, Google, and Microsoft, have been hacked (Schmitt 2019). Another relevant question is whether companies that monitor traffic would be motivated to spend a large amount to protect privacy. The number of privacy violations already happening indicates that many companies have not been motivated to prioritize protection of privacy unless required to do so by government regulation. A challenging question is therefore: How can governments hold companies monitoring vehicles financially liable for privacy violations?

In summary, only high-capacity attackers, such as states and state-supported groups, will be able to cause large traffic accidents. The question is whether such actors will be motivated to conduct such attacks. Promoting division, distrust, and doubt in "enemy" countries is already very common (Linvill and Warren 2019). It is therefore plausible that high-capacity attackers may want to create distrust in the transport system. It is more uncertain whether very many high-capacity attackers would want to cause deaths and serious injuries, partly because of the risk of being exposed as the attacker and thereby suffering reputational damage.

Hence, high-capacity attackers will have both the resources and the motivation to cause incidents that create distrust of the transport system. Some high-capacity attackers might also be willing to cause deaths and serious injuries to create distrust of the transport system.

Paralysis of the transport system

Sometimes countries have outstanding issues that they experience as so salient that they prefer to wage war. Conducting a cyberattack can be easier and less risky than military action. Cyberattacks can be an especially convenient alternative when the countries in question are located far from each other.

Since it is possible to compromise all vehicles of a specific brand through an over-the-air update, the manufacturer should be motivated to prioritize investing in cybersecurity of update servers. It is therefore not plausible that actors with medium-to-low capacity will manage to hack an update server. However, even if manufacturers prioritize cybersecurity, they will probably not be able to stop high-capacity attackers. Even hi-tech companies, such as Apple, Google, and Microsoft, have experienced that their software update infrastructures have been hacked (Schmitt 2019).

In summary, the scenario on paralysis of the transport system is plausible. For states, conducting such cyberattacks can be an attractive alternative to military action. Prioritizing protecting update servers from such attacks will make it less probable that hackers succeed in attacking, but will not stop the most determined high-capacity attackers.

Risk situation

In this analysis, we have included six scenarios: four scenarios where the attacker needs only limited capacity and two scenarios that only high-capacity attackers could realistically conduct. The scenarios "playful teenagers," "kidnapping for ransom," and "domestic abuse" demonstrate that it might be difficult to stop all unauthorized takeovers of autonomous vehicles, especially by people who have access to the vehicle owner's property. Two important prevention measures that will either mitigate the worst consequences or make it more difficult to maliciously use the vehicles are to make it difficult to manipulate vehicles' speeds and to protect individual data about travel patterns, respectively.

The fourth scenario, "autopilot manipulation," requires very little technical knowledge and it will not be possible to remove all possibilities of autopilot manipulation. Most environmental organizations will, fortunately, prefer to cause no deaths of or injuries to vehicles' passengers. To ensure that autopilot manipulation does not cause deaths or injuries among passengers, it is necessary to include safety measures in the vehicles to protect passengers' bodies in any traffic accident.

The last two scenarios, "large traffic accident" and "paralysis of the transport system," require high-capacity attackers. The number of potential high-capacity attackers is much lower than the number of low-capacity attackers and attempted attacks will therefore probably be rare. To prevent all such attacks, however, will probably be impossible. Measures that limit the consequences of such attacks will therefore be necessary. Such measures include safety measures in vehicles to protect the occupants in traffic accidents and measures that make vehicles easier to remove in case they do not function. The last category of measures includes installing kill switches that make it possible to turn off the vehicle manually, thus overriding the autopilot

(Consumer Watchdog 2019) and making the vehicle possible to move by four fit adults when it is turned off manually.

Conclusion

Forecasting cybercrimes against a transport system that is under continuous development is difficult and could be seen as a speculative exercise. In this paper we try to circumvent this problem by employing a method of risk analysis that has been developed to avoid using probability. A possible disadvantage of the method is its emphasis on worst-case scenarios at the expense of less serious, but more probable, scenarios. Including scenarios where the attackers have different levels of technical skills and capacities may help us avoid this pitfall.

The analysis included six scenarios: joyriding, kidnapping, domestic abuse, autopilot manipulation, large transport accident, and paralysis of the transport system. Spending resources on cybersecurity should make it possible to increase the difficulty and, thus, increase the skill level required to successfully conduct such attacks. That greater difficulty would deter some would-be attackers and make other would-be attackers unsuccessful in their attempts. To ensure that vehicle developers invest enough to successfully prevent most would-be attackers, developers must have the necessary incentives and be held liable for successful cyberattacks. It might, however, be impossible to prevent all such attacks. Measures that limit the consequences of successful cyberattacks will therefore also be necessary. Such measures include safety measures in vehicles to protect occupants in traffic accidents and measures that make vehicles easier to remove in case they do not function.

This security risk analysis emphasizes cyberattacks that might threaten the functioning of the transport system rather than less serious but more frequent cyberattacks. Petty cybercrimes that are not serious enough to threaten the transport system, but might still cause large costs to society because of such crimes' frequency, are therefore not included here. To counter this bias against petty cybercrimes and to detect new trends in cyberattacks against the transport system, this analysis should be supplemented by the collection and systematization of vulnerability exploitations against different elements of the transport system.

Acknowledgements We have received valuable comments and advice from Henrik Larsen and Fredrik Walløe. We thank the European Union for funding this study.

Authors' contributions Sunniva Meyer and Rune Elvik contributed to the study's conception and design. Information gathering and analysis were performed by Sunniva Meyer and Espen Johnsson. The first draft of the manuscript was written by Sunniva Meyer and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open access funding provided by Institute Of Transport Economics. This study was funded by the EU-funded (Horizon 2020) project Levitate ("Societal Level Impacts of Connected and Automated Vehicles").

Data availability Not applicable.

Code availability Not applicable.

Declarations

Conflicts of interest/Competing interests The first author is an unpaid member of the committee SNK 296 Societal Security in Construction, Civil Engineering and Real Estate/Standards Norway, which prepared the Norwegian Standard for Security Risk Assessment (NS 5832:2014).

References

Bird J (2019) Car hacking threatens vision of connected mobility. Financial Times. https://www.ft.com/content/163f08c6-6ce3-11e9-9ff9-8c855179f1c4. Accessed 30 Jul 2019

Boyd C (2018) IoT domestic abuse: What can we do to stop it? https://blog.malwarebytes.com/cybercrime/2018/07/iot-domestic-abuse-can-stop/. Accessed 30 Jul 2019

Buttice C (2019) Hacking autonomous vehicles: Is this why we don't have self-driving cars yet? Techopedia. https://www.techopedia.com/hacking-autonomous-vehicles-is-this-why-we-dont-have-self-driving-cars-yet/2/33650. Accessed 31 Jul 2019

Campbell P (2018) Hackers have self-driving cars in their headlights. Financial Times. https://www.ft.com/content/6000981a-1e03-11e8-aaca-4574d7dabfb6. Accessed 31 Jul 2019

Cho KT, Kim Y, Shin KG (2018) Who killed my parked car? arXiv.org. arXiv:1801.07741

Claburn T (2018) Newsflash: Car cyber-security still sucks. The Register. https://www.theregister.co.uk/2018/01/26/car_hacking_wireless/. Accessed 30 Jul 2019

Consumer Watchdog (2019) Kill switch. Why connected cars can be killing machines and how to turn them off. Consumer Watchdog. https://www.consumerwatchdog.org/report/kill-switch-why-connected-cars-can-be-killing-machines-and-how-turn-them. Accessed Aug 2019

Dalton RJ, Recchia S, Rohrschneider R (2003) The environmental movement and the modes of political action. Comp Political Stud. https://doi.org/10.1177/0010414003255108

Doffman Z (2019) State-sponsored cyberattacks 'challenge the very concept of war'. Forbes. https://www.forbes.com/sites/zakdoffman/2019/08/10/state-sponsored-cyberattacks-challenge-the-very-concept-of-war-report/?sh=182ab67b54d6. Accessed Aug 2019

Ekblom P (2017) Crime, situational prevention and technology: the nature of opportunity and how it evolves. In: McGuire MR, Holt TJ (eds) The Routledge handbook of technology, crime and justice. Routledge, London, pp 353–374

Felson M, Eckert MA (2018) Crime and everyday life: a brief introduction. SAGE Publications, Thousand Oaks

Furnell S (2017) The evolving landscape of technology-dependent crime. In: McGuire MR, Holt TJ (eds) The Routledge handbook of technology, crime and justice. Routledge, London, pp 65–77

Goodin D (2018) A $225 GPS spoofer can send sat-nav-guided vehicles into oncoming traffic. Ars Technica. https://arstechnica.com/information-technology/2018/07/a-225-gps-spoofer-can-send-autonomous-vehicles-into-oncoming-traffic/. Accessed Aug 2019

Graham RS, Smith SK (2019) Cybercrime and digital deviance. Routledge, New York

Hawkins AJ (2019) Tesla didn't fix an autopilot problem for three years, and now another person is dead. The Verge. https://www.theverge.com/2019/5/17/18629214/tesla-autopilot-crash-death-josh-brown-jeremy-banner. Accessed Aug 2019

Hull R (2019) A car is stolen EVERY 5 MINUTES in Britain: Vehicle thefts up 50% in 5 years thanks to criminal gangs hacking keyless systems and reduced policing. This is Money. https://www.thisismoney.co.uk/money/cars/article-6631925/Vehicle-thefts-risen-50-5-years-Home-Office-figures-show.html. Accessed Aug 2019

Jore SH (2019) Standardization of terrorism risk analysis. In: Olsen OE, Juhl K, Lindøe PH, Engen OA (eds) Standardization and risk governance. Routledge, London, pp 150–166

Li Y, Tu Y, Fan Q, Dong C, Wang W (2018) Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. Accid Anal & Prev. https://doi.org/10.1016/j.aap.2018.09.016

Linvill D, Warren P (2019) That uplifting tweet you just shared? A Russian troll sent it. Rolling Stone. https://www.rollingstone.com/politics/politics-features/russia-troll-2020-election-interference-twitter-916482/. Accessed Dec 2019

Malwarebytes (2019) What is hacking? Malwarebytes. https://www.malwarebytes.com/hacker/. Accessed 31 Jul 2019

Moore R (2014) Cybercrime: investigating high-technology computer crime. Routledge, New York

Newton A (2016) Crime, transport and technology. In: McGuire MR, Holt TJ (eds) The Routledge handbook of technology, crime and justice. Routledge, London, pp 281–294

Office of the Chairman of the Joint Chiefs of Staff (2019) DOD dictionary of military and accociated terms (July 2019). Joint Chiefs of Staff, Washington DC

Osborne C (2018) The most interesting internet-connected vehicle hacks on record. ZDNet. https://www.zdnet.com/article/these-are-the-most-interesting-ways-to-hack-internet-connected-vehicles/. Accessed Aug 2019

Pogue C (2018) The 2018 black report. Decoding the minds of hackers. Nuix, Sydney

Sanguino TDJM, Domínguez JML, Baptista PDC (2020) Cybersecurity certification and auditing of automotive industry. In: Milakis D, Thomopoulos N, van Wee B (eds) Policy implications of autonomous vehicles, vol 5. Cambridge, Elsevier, pp 95–124

Schmitt B (2019) Top OTA expert shows how state actors hack into your car and what happens next: 'People will die'. The Drive. https://www.thedrive.com/tech/29120/top-ota-expert-shows-how-state-actors-hack-into-your-car-and-what-happens-next-people-will-die. Accessed Aug 2019

Sektorstyret BAE (2010) Revidert mandat for komité SN/K 296 - Samfunnssikkerhet i BAE sektoren. Standard Norge, Oslo

Soare B (2019) Are hackers threatening the adoption of self-driving cars? And all about the current state of autonomous vehicles, Heimdal Security. https://heimdalsecurity.com/blog/hackers-self-driving-cars/. Accessed 31 Jul 2019

Standard Norge (2013) Regler fra Standardiseringsarbeidet. Vedtatt av Standard Norges styre 2013-08-27. Standard Norge, Oslo

Standard Norge (2021) Standards Norway. Standard Norge. https://www.standard.no/en/toppvalg/about-us/standards-norway/#.YMNehb7itnI. Accessed June 2021

Tencent Keen Security Lab (2019) Experimental security research of tesla autopilot. Keen Security Lab Blog. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf. Accessed Aug 2019

Thomson I (2018) Say what you will about self-driving cars - the security is looking 'OK'. The Register. https://www.theregister.co.uk/2018/08/10/autonomous_car_hacking/. Accessed Aug 2019

Virta S (2019) Pre-crime and standardization of security risks. In: Olsen OE, Juhl K, Lindøe PH, Engen OA (eds) Standardization and risk governance. Routledge, London, pp 137–149

Von Solms R, van Niekerk J (2013) From information security to cyber security. Computers & Security. https://doi.org/10.1016/j.cose.2013.04.004

Zamora W (2018) Under the hoodie: Why money, power, and ego drive hackers to cybercrime. Malwarebytes. https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/. Accessed 30 Jul 2019