‘Connected’ auto’s, een andere aanpak van criminaliteit

december 2016

AVc

Stichting Aanpak Voertuigcriminaliteit

INHOUDSOPGAVE

MANAGEMENTSAMENVATTING

‘Connected’ auto’s, een andere aanpak van criminaliteit

Om in de toekomst succesvol te blijven in de aanpak van voertuigcriminaliteit is in de zomer van 2016 een verkennende notitie gemaakt omtrent de ontwikkelingen van connected personenvoertuigen die ook semi-autonome functies hebben. Door middel van interviews en deskresearch is een integraal beeld gevormd dat in deze notitie weergegeven is. Hierbij komen onderwerpen aan de orde zoals de connected car als onderdeel van het Internet of Things en in het bijzonder in de veranderende mobiliteitswereld. Verder wordt bezien welke kansen en uitdagingen connected voertuigen bieden voor de aanpak van voertuigcriminaliteit, om tot slot aanbevelingen te geven met betrekking tot de rol van AVc in deze.

Internet of Things

Een nieuwe industriële revolutie is gaande. Met het volwassen worden van internet en de komst van vele connected devices, zoals auto’s, worden andere businessmodellen mogelijk die de klant en zijn behoeften meer centraal stellen. Dit dwingt tot anders denken: van productlife- naar servicelife cyclemanagement. Dit biedt kansen voor nieuwkomers in gevestigde industrieën. Dit biedt ook kansen voor criminelen. Het veilig laten verlopen van de vele datastromen uit de diverse devices is een uitdaging. De zwakste schakel in de gehele keten bepaalt immers de veiligheid. De ontwikkelingen gaan sneller dan verwacht, waardoor er soms te weinig aandacht is voor security. Daarnaast zijn bedrijven in de keten zich nog onvoldoende bewust van de gevaren van cybercrime en wordt er nog weinig proactief op geïnvesteerd. Tevens is er een grote schaarste aan cyberspecialisten, worden de cybercriminelen steeds beter en zijn hacktools op internet ruimschoots voorhanden. Jaarlijks wordt de totale schade van cybercrime in alle sectoren geschat op 325 miljard euro wereldwijd.

Veranderende wereld van mobiliteit

Twee belangrijke drijfveren voor verandering in de auto-industrie zijn overheidsbeleid (richting milieu en veiligheid) en consumentenvraag. Nieuwe mobiliteitssystemen ontstaan in diverse vormen zoals: carsharing (Car2Go), ridehaling (Uber), ridesharing (Blablacar), microtransit (VIA), Mobility as a Service (Moovel) en op termijn gedeelde autonome voertuigen (Google, Ford). In het algemeen geldt dat, door gebruik van connectiviteitsfuncties, mobiliteit op aanvraag en op korte termijn te verkrijgen is. De grenzen tussen OV en privaat vervoer en tussen bezit en gebruik gaan meer vervagen. Informatie uit het voertuig is echter essentieel om grip te houden op en sturing te geven aan het gebruik van het voertuig. De benodigde data, zoals locatiedata, wordt veelal door een blackbox (telematica unit) ontsloten. Deze is aangesloten op de OBD II (On Board Diagnostic) poort in het voertuig.
Autofabrikanten gaan nieuwe samenwerkingen aan met o.a. telecommunicatiebedrijven en hightechbedrijven om de 'rijdende computer' te kunnen bouwen. Ze hebben veiligheid hoog in het vaandel staan en leveren dan ook in toenemende mate ondersteunende rijfuncties, zoals bijvoorbeeld automatisch inparkeren en automatisch remmen. Omdat voor de systeemintegratie die alle connectiviteitdiensten vragen, de huidige CANbus uit de jaren '80 niet ontworpen is, werken ze ondertussen aan een compleet vernieuwd data netwerk in de toekomstige auto.
De Nederlandse overheid heeft de ambitie Europees koploper te zijn in het gebruik van Intelligente Transport Systemen. Door de toepassing van informatie- en communicatie technologie in voertuigen (sensoren en zelfrijdfuncties) en zogenaamde wegkantsystemen wordt het mogelijk het verkeer veiliger, efficiënter, betrouwbaarder en milieuvriendelijker te maken. Voor een veilig dataverkeer is het onder meer belangrijk dat voertuigen altijd kunnen worden geïdentificeerd, dat geverifieerd wordt of een bericht daadwerkelijk afkomstig is van de wegbeheerder en vice versa, en of een bericht authentiek is. Een Public Key Infrastructure hiervoor is momenteel in ontwikkeling.

Kwetsbaarheden van connected voertuigen

De verhoogde connectiviteit van auto's brengt reële cybersecurityrisico's met zich mee. In tegenstelling tot de meeste consumentenproducten kan een inbreuk op een auto immers gelijk levensbedreigend zijn. Via de OBDII poort kunnen externe systemen voor navigatie (USB, CD, Updatesoftware), verkeersinformatie, entertainment (Spotify) en handsfreefuncties als remote control aangesloten zijn of worden. Deze aansluitingen bieden relatief eenvoudig toegang tot de CANbus, waarmee o.a. de controle over de motor, de besturing, de remmen en andere kritische onderdelen van een voertuig zijn over te nemen. Ook kan data gemanipuleerd worden of zelfs worden gestolen. 'White hat hackers' tonen aan dat hier de zwakste schakel zit en motiveren autofabrikanten en toeleveranciers om haast te maken met betere beveiliging. Op dit moment is de connected auto nog geen doelwit van georganiseerde cybercrime. Naar verwachting zal in 2020 75% van de auto's een vorm van connectiviteit hebben.

De groei wordt mede gestimuleerd door de groeiende vraag van consumenten naar andere (connected) mobiliteitsvormen, de invoering van eCall in 2018 en de ITS doelen van de overheid. De aantallen die daarmee ontstaan, vormen naar verwachting een lucratieve basis voor cybercriminelen.

Internet of Insecure Things

De consument moet er blijvend op kunnen vertrouwen dat een voertuig veilig is. De cybersecurity problematiek van auto's staat niet op zichzelf, maar in de reeks van devices aangesloten op internet. Cybersecurity werkt pas als het 'end to end' in de gehele bedrijfskolom aandacht krijgt. Als cybersecurity niet is geregeld, dan is privacy ook niet geregeld en wordt het een belangrijke belemmering voor innovaties. Mede daarom heeft de Europese Commissie recent de zogenaamde NIS richtlijn vastgesteld die als doel heeft de veiligheid van netwerken en informatiesystemen te verbeteren middels een gecoördineerde aanpak van cybercrime. In Nederland is de Wet Computercriminaliteit III in de maak, de zogenaamde 'terughackwet'. Deze wet biedt opsporingsinstanties grotere mogelijkheden en het Openbaar Ministerie de mogelijkheid hogere straffen te eisen. Het Nationaal Cyber Security Centrum geeft nationale ondersteuning op het vlak van digitale veiligheid.

Veranderende wereld van de AVc deelnemers

Bovengenoemde ontwikkelingen raken de deelnemers van AVc.
De Nationale Politie stoomt haar organisatie klaar voor de bestrijding van een groeiend aantal cybercrime delicten. Het Landelijk Innovatieteam Automotive doet onderzoeken naar tactieken en technieken op het gebied van connected voertuigen. Een eerste resultaat daarvan is de recente start met het uitlezen en analyseren van de data uit de Event Data Recorder (onderdeel blackbox) bij ernstige auto ongelukken om de eventuele schuldvraag beter vast te kunnen stellen.
Het Verbond van Verzekeraars oriënteert zich op de innovaties en de daarbij mogelijke businessmodellen. Connected voertuigen maken het mogelijk om 'Insurance as a Service' aan te bieden, waarbij de gebruiker betaalt afhankelijk van zijn rijgedrag (UBI) of een directe autoverzekering, waarbij de schade zonder schuldvraag (vergelijk een gezondheidsverzekering) verzekerd is. Voertuigen dienen daarvoor een telematica unit aan boord te krijgen, waarmee zogenaamde track en trace functionaliteit gemeengoed kan worden.
De RDW rondt eind 2016 haar programmaplan VICTOR af. Dit plan is een verkenning om kennis en ervaring op te doen rond Intelligente Transport Systemen. Voor de RDW betekent dit mogelijk een omslag van een fysieke Europese typegoedkeuring voor toelating van een voertuig op de weg naar een continue landelijke softwarecertificering van een voertuig. Een geüpdatet auto moet immers ook na de update weer voldoen aan de eisen. Bij het ontwerpen van de infrastructuur voor dit soort configuratiebeheer wordt cybersecurity nadrukkelijk geadresseerd.
Het ministerie van Veiligheid en Justitie heeft hacking en diefstal als beleidsterrein. Er lijkt echter nog geen interdepartementaal overleg met betrekking tot cybercrime in connected voertuigen te zijn met bijvoorbeeld het Ministerie van Infrastructuur en Milieu.

BOVAG en RAI Vereniging lijken door de autofabrikanten nog weinig geïnformeerd te worden over de connectiviteit van voertuigen, anders dan noodzakelijk om connectiviteitsdiensten als merk gelieerde service te verkopen. Dit vertaalt zich ook terug in de showroom; kennis van rij ondersteunende functies en connectiviteitsfuncties behoeft aandacht.
ANWB lijkt zich (inter-)nationaal goed voor te bereiden op haar belangenbehartigingsrol en haar commerciële kansen bij connected voertuigen voor de leden. Met het testen van telematica units en bigdata analyses doen ze ervaring op. Ondanks dat ze zelf zeggen ‘many questions, few answers’ staat security hoog op de agenda.
TLN behartigt de belangen van de logistieke sector. Ook daar spelen de onderhavige ontwikkelingen een belangrijke rol. De sector heeft reeds de nodige ervaring opgedaan met het beheer van een connected vloot. Deze ervaring kan zeker in bredere zin worden benut.
ARN bereidt zich voor op de gevolgen van de veranderende mobiliteit voor het recycleproces. Vooralsnog gaat dit over veranderend materiaalgebruik als composieten en geavanceerde elektronica. Of ARN in de toekomst ook rijdende computers gaat slopen en hoe het dan zit met de security is nog niet gezegd.

Conclusies en aanbevelingen aan AVc

Het aantal voertuigen dat op enige wijze connected is, neemt de komende jaren snel toe. Dit biedt goede kansen voor identificatie van het voertuig. Voertuigen produceren veel data die voor veel partijen, anders dan de fabrikant, interessant is. Ook voor de aanpak van voertuigcriminaliteit biedt deze ontwikkeling kansen. De discussie rondom zeggenschap over data en privacy wordt echter nog volop gevoerd en aan wetgeving wordt gewerkt op nationaal en internationaal niveau. Ondertussen werken de fabrikanten steeds meer samen met toeleveranciers om toekomstige innovatieve oplossingen te bieden voor hun voertuigen als rijdende computers. Het rijdend park en de nieuwe voertuigen van de komende jaren baren echter ook zorgen. White hat hackers tonen in toenemende mate aan dat huidige connected voertuigen niet cybersecure zijn. Dit vraagt een end to end security aanpak, die nieuwe toeleveranciers en mobiliteitsproviders een integraal onderdeel maakt van de veiligheid van een voertuig. Aanbevolen wordt om security hoger op de agenda te zetten door de ontwikkelingen te volgen en daarbij waar mogelijk aan te sluiten bij de diverse ontwerpprocessen als C-ITS (Connected en Coöperatieve Intelligente Transport Systemen), een thema binnen Beter Benutten van het ministerie van I&M. Aandacht voor zaken als standaardisering en certificering is van groot belang. Ook moet worden gekeken naar de meerwaarde van de ‘levenscyclusbenadering’. Op vele plaatsen in de automotive kolom kan security aandacht krijgen en veilig gesteld worden. Hiervoor is echter eerst bewustzijn van het criminaliteit-element bij de ontwikkelingen binnen de mobiliteitssector nodig. Dit geldt zowel voor de branche als voor de consument. Security is geen sexy onderwerp.

Om voldoende aandacht te krijgen kan het adresseren van de uitdaging ook worden verbonden aan het element privacy: Geen privacy zonder security! Breng ook partijen met elkaar in contact en faciliteer kennisdeling. Betrek in dit kader mogelijk nieuwe deelnemers bij AVc en maak ze deelgenoot van pilots enz. Kijk ook internationaal, probeer te leren van ontwikkelingen elders (andere sectoren als ICT, maar ook op dit domein in bijvoorbeeld de VS). Zet in op een versterking/ontwikkeling van publiek-private opsporing. Connected voertuigen zijn immers beter traceerbaar en deze kans kan optimaal benut worden. Benut hierbij ook de kansen die voortvloeien uit verscherpte wetgeving rondom datamisbruik/hacking. En last but not least, stel een expertgroep samen die ondersteuning biedt aan de scoping van AVc, haar deelnemers en de implementatie van de aanbevelingen.

INLEIDING

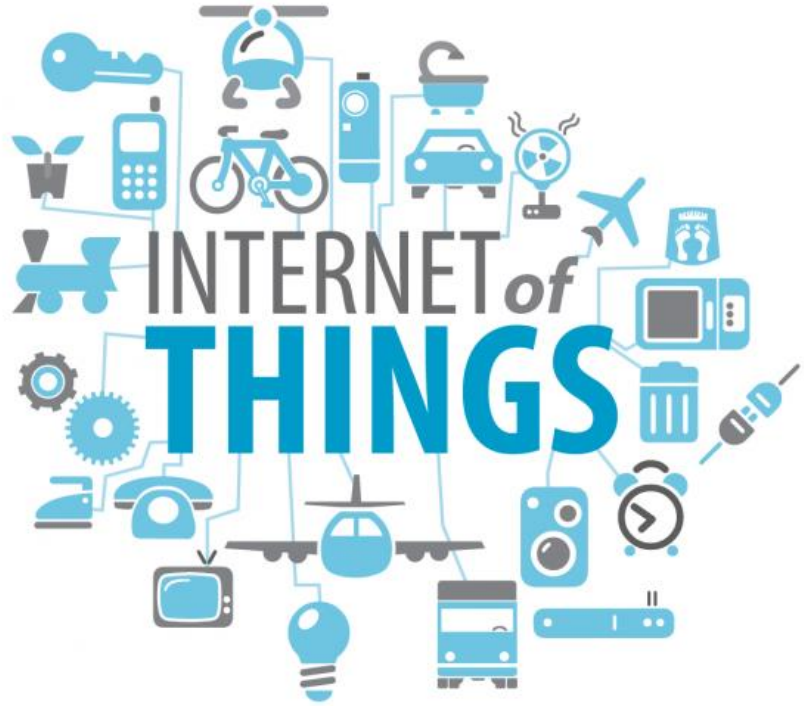
Stichting Aanpak Voertuigcriminaliteit (hierna AVc) ziet een verdere daling van het aantal autodiefstallen. Op basis van de huidige cijfers verwacht de organisatie dat het er dit jaar minder dan tienduizend zullen zijn. Vooral auto's tot drie jaar worden minder gestolen. Betere beveiligingssystemen waarmee auto's af fabriek worden uitgerust en intensievere internationale samenwerking werpen hun vruchten af. AVc geeft aan dat landen steeds meer gegevens uitwisselen, waardoor het voor de autodief lastiger wordt om gestolen voertuigen te her-registreren.

Om in de toekomst de aanpak van voertuigcriminaliteit succesvol te blijven garanderen is een verkennende notitie gemaakt omtrent de ontwikkelingen van connected personenvoertuigen die vaak ook semi-autonoom kunnen rijden. Welk onderdeel deze auto's vormen in de connected wereld en in het bijzonder in de veranderende mobiliteitswereld. Welke kansen en uitdagingen dat biedt voor de aanpak van voertuigcriminaliteit om tot slot te kunnen bepalen welke rol AVc hierin kan vervullen.

Om een beeld te vormen van de kansen en bedreigingen die connected voertuigen bieden voor de aanpak van voertuigcriminaliteit zijn over een breed spectrum interviews gehouden en is deskresearch gedaan. In deze notitie worden diverse geraadpleegde rapporten en artikelen via een hyperlink in de tekst weergegeven.

1. INTERNET OF THINGS

Informatie Technologie maakt bedrijfsmodellen mogelijk die voorheen ondenkbaar waren. Complete industrieën dreigen te worden opgegeten en nieuwkomers op de markt verschijnen uit een onverwachte hoek. Er wordt gesproken van een nieuwe industriële revolutie. Voor een groot gedeelte wordt deze digitale disruptie veroorzaakt door de Internet of Things, hierna te noemen IoT. Nederland neemt wereldwijd de vijfde plaats in als het gaat om aantal aan internet verbonden devices per hoofd van de bevolking na resp. Korea, Denemarken, Zwitserland en Verenigde Staten. Nederlandse organisaties zijn echter nog niet volwassen in cybersecurity. In de benodigde omslag van ouderwetse *preventie* naar *detectie* en *respons* wordt nog te weinig geïnvesteerd. De Meldplicht Datalekken die begin van 2016 is gestart, dwingt ook tot snel kunnen melden en dus tot detecteren. Onderzoeksbureau Gartner verwacht dat in 2020 een kwart van de cybercrime via IoT plaatsvindt. Zij pleiten voor een verhoging van het beveiligingsbudget. Als er ergens geldt 'dat stilstand achteruitgang is' dan is dat wel bij cybersecurity.



De vraag naar cybersecurity specialisten is groter dan het aanbod. In 2019 wordt wereldwijd een tekort van 1 miljoen cybersecurity-experts verwacht, wat organisaties en landen nog kwetsbaarder maakt. Hacking challenges zouden dit tekort mede kunnen voorkomen. Ze zijn naast een goede vingeroefening een methode om kennis op te doen en toolsets te leren gebruiken, nieuw talent te spotten en te netwerken. Het tekort aan security kennis heeft direct invloed op de bedrijven. Het leidt tot directe en meetbare schade zoals dataverlies en inbreuk op intellectueel eigendom. Bedrijven worstelen in hun directies met het vormgeven van cybersecurity in hun organisatie. Een Chief Information Security Officer met mandaat kan het verschil maken in de boardroom. Hierbij wordt verwezen naar het rapport van KPMG over ‘Vijf denkfouten over cybersecurity’.

Even de praktijk; White hat hackers hebben ransomware geïnstalleerd op een slimme thermostaat die eerst de temperatuur in huis opvoert tot 37 graden en daarna vraagt om een PIN-code om de thermostaat te ontgrendelen. De PIN-code verandert elke halve minuut en voor het opvragen moet steeds een bitcoin worden betaald. Dit maakt goed duidelijk hoe criminelen de komende jaren het IoT kunnen gaan beheersen. Alle in netwerken verbonden apparatuur die zwakheden bevat, vormt een potentieel doelwit. Bedrijven en consumenten dienen zich hier beter bewust van te worden. Denk onder meer aan beveiligingssystemen, connected auto’s, slimme koelkasten, televisies, printers, wearables en per app bedienbare LED lampen. Gevoelige informatie die over het wifi-net gaat, is eenvoudig op te vangen door criminelen.

Het IoT-beveiligingdrama voltrekt zich als voorspeld. IoT ontwikkelaars ondermijnen massaal de veiligheid van internet vanwege het gemak van het gebruik van zogenaamde default sleutels en bestaande certificaten, de gewenste snelle time to market en de prijsdruk. Verwacht wordt dat in toenemende mate onderdelen van IoT het doel worden van de makers van ransomware. Sensoren kunnen bijvoorbeeld besmet worden, waarna de legitieme gebruiker niet meer bij de meetgegevens kan (datalocker), tenzij hij betaalt of niet meer in zijn computer of device kan (computerlocker). Symantec schreef hier een whitepaper over.

2. VERANDERDE WERELD VAN MOBILITEIT

2.1 De consument

De auto-industrie verandert en zal in een stroomversnelling komen, omdat de consument anders naar mobiliteit kijkt. Zo bewijst de groeiende vraag naar bedrijfsmodellen, als ‘Car-as-a-Service’ en autodelen (een stijging van 300 procent in 2 jaar) dat de auto vaker als dienst wordt beschouwd. Dit leidt tot een verschuiving van eigendom, een hogere bezettingsgraad en daardoor een kortere levensduur van auto’s.
De twee belangrijkste drijfveren voor verandering in de auto-industrie zijn veelal overheidsbeleid en de vraag van consumenten. Overheidsbeleid heeft de auto-industrie altijd beïnvloed en gezorgd voor een push richting milieu- en veiligheidsbewustzijn. De pull van consumenten wordt steeds sterker als drijvende kracht achter verandering in de auto-industrie. Consumenten vragen om steeds meer diensten en de nieuwste technologie in hun voertuigen, waardoor auto’s ‘smartphones op wielen’ worden. Aspecten als veiligheid, zelfsturend rijden en infotainment hebben zo langzamerhand meer invloed op het koopgedrag dan merkimago, motorcapaciteit en betrouwbaarheid. Ook zijn consumenten bereid om meer te betalen voor deze functionaliteiten. De ontwikkelingen gaan sneller dan automotive-analisten drie tot vijf jaar geleden hadden voorspeld. Het aantal intelligente en actieve systemen in voertuigen neemt in rap tempo toe.

De complexiteit van de hoog-autonome en straks zelfrijdende auto's neemt hiermee toe. Het waarborgen van een correcte, geautomatiseerde werking van het voertuig wordt daarmee cruciaal. In potentie neemt het aansprakelijkheidsrisico van de bestuurder af en het productrisico voor de fabrikant toe. Een aantal fabrikanten overweegt nu al om een deel van het risico van het voertuig af-fabriek mee te verzekeren bij verkoop en levering. De toename van de complexiteit geldt ook voor het schadeherstel. Waarborging van correcte werking van het voertuig zal plaatsvinden bij aangewezen specialistische schadeherstellers. Specialisten die naast herstel en kalibratie van onderdelen, ook in staat zijn om de technische en functionele werking van de auto te garanderen. Een soort verplichte winkelnering waarbij het merk verzekering en schadeherstel bepaalt. Eigenaren van voertuigen zullen tevens verleid worden om de auto op basis van data afhankelijk van het ge- en verbruik te laten onderhouden en naar de laatste softwareversie te updaten.

Een model van gebruik, service, onderhoud en herstel vanuit één entiteit, dat gangbaar is voor steeds meer consumentenelektronica. Een model waarvan ook een merk als Volvo reeds heeft aangegeven: 'Schadeherstel en verzekeren van autonoom rijdende auto's gaan we echt zelf doen'. Op welke wijze en met welk tempo vinden de ontwikkelingen van de volledig autonome voertuigen nu echt plaats? De autofabrikanten drukken de kaarten stevig tegen de borst en zijn voorzichtig in het noemen van tijdslijnen. Tot drie jaar terug werd een introductie tussen 2025 en 2030 gezien als een utopie. Momenteel koersen vrijwel alle automerken af op 2021 of al eerder! Maar zover is het nog niet. Bestaande voertuigen gaan immers nog tien tot twintig jaar mee. Het wagenpark zal nog zeker twintig jaar lang een mix zijn van traditionele, hoog autonome en volledig zelfrijdende auto's.
Ondertussen nemen de technologie en wireless functies toe en ontstaan er allerlei nieuwe mobiliteitsvormen als carsharing (bv Car2Go) ridehaling (Uber), ridesharing (Blablacar), microtransit (Via), Mobility as a Service (Moovel) en op termijn gedeelde autonome voertuigen (Google, Ford). In zijn algemeenheid geldt dat mobiliteit op korte termijn verkrijgbaar is, op aanvraag beschikbaar en dat toegang tot een auto via connectiviteitsfuncties verkregen kan worden. Hiermee vervagen de grenzen tussen publieke (OV) en privaat vervoer en eveneens de grenzen tussen eigendom of delen van gebruik. Dit biedt een complete verandering van vervoeren met allerlei mogelijkheden om bijvoorbeeld op parkeren, verkeersstromen en OV meer grip te krijgen. En hiermee de first en de last miles beter in te regelen of de piektijden te ontlasten of antidiefstaltips in apps te integreren. Voor autofabrikanten (OEM) betekent dit nieuwe businesspartners.

Bewegingen als ‘van autobezit naar autodelen’ en multimodaal vervoer worden met name in verstedelijkte gebieden gezien. Het aantal deelauto’s in Nederland bedraagt in 2015 ongeveer 11.200. Dat is 0,1% van het totale wagenpark. De groep deelauto’s bestaat voor een deel uit de vloten van bedrijven als Greenwheels, Car2go en ConnectCar. Daarbij gaat het in totaal om ongeveer 2.450 auto’s in Nederland, vooral in Amsterdam en Utrecht. Deze vloten zijn afgelopen jaren opgebouwd maar groeien nu nauwelijks. De overige deelauto’s zijn voor het merendeel auto’s van particulieren, die via platforms als SnappCar en MyWheels gedeeld worden met anderen. Dit fenomeen groeit wel. Door middel van een app kan toegang gekregen worden tot het voertuig. Ook alternatieve leasevormen als een mobiliteitsbudget, shortlease of verhuur zijn groeiend. Private lease groeit hard en wordt voor 2015 geschat op 35.000 nieuwe voertuigen . Informatie uit het voertuig wordt belangrijk om grip te houden op gebruik, e(mergency)Call, B(reakdown)Call en S(ervice)Call. Dit betekent een forse toename van de noodzaak tot connected zijn van het voertuig door veelal het gebruik van een blackbox.

De Amerikaanse National Highway Traffic Safety Administration (NHTSA) heeft vier niveaus van autonoom rijden gedefinieerd.
Het gaat om:

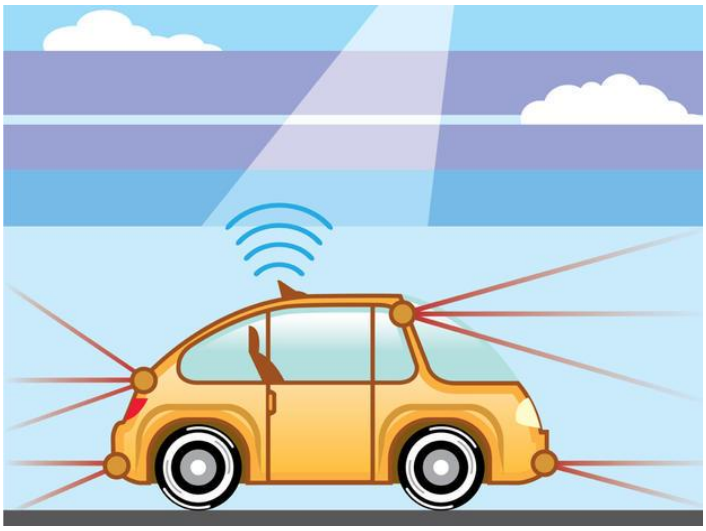
- de bestuurder die alle controle heeft over het voertuig
- een semi-autonoom voertuig met gebruik van ADAS (Advanced Driver Assistance Systems) functies
- een volledig autonoom voertuig (een Tesla in 2018)
- een autonoom voertuig zonder opties om als mens te rijden; dus zonder stuur.

2.2 De autofabrikanten

De strategieën van veel autofabrikanten zijn gericht op het ontwikkelen van connected car-technologieën en -diensten door inzet van cloud computing, bigdata en Internet of Things. De meest aangeboden diensten zijn milieu, nieuws en/of navigatie gerelateerd. Rij-assistentie en veiligheidsdiensten (het volgen van een gestolen voertuig) zijn opkomend. Sommigen werken al aan afrekensystemen in het voertuig. Autofabrikanten kunnen deze uitdagingen niet in hun eentje aan. Ze zullen voor hun behoefte aan innovatie steeds meer op toeleveranciers leunen, om zo toegang te houden tot technologie en know-how op het gebied van R&D en engineering. Momenteel ontwikkelen en monteren toeleveranciers ca. 65% van de gemiddelde waarde van een voertuig en 55% van de innovaties bij toeleveranciers komen uit Nederland.

Fabrikanten maken zich ondertussen zorgen over de beveiliging, het gebrek aan standaarden en de integratie van verschillende technologieën en ecosystemen van diverse dienstverleners. Verwacht wordt dat in 2020 75% van de geproduceerde auto's een vorm van wireless connectiviteit heeft.

In tegenstelling tot bijvoorbeeld een merk als Tesla (of toekomstige Apple/Googlecars) zijn de meeste auto's nooit ontwikkeld als rijdende computers. De CANbus (interne datasnelweg in de auto) stamt uit de jaren tachtig en lijkt op een grote spaghetti van software, vergelijkbaar met de oude mainframesoftware. Dit is ontstaan door toevoeging van steeds meer elektronische functionaliteiten met in het begin Fuel Injection, Airbags, ABS, navigatie, centrale deurvergrendeling, climatcontrol, cruisecontrol, automatisch inklapbare spiegels en ESP. En nu de specifieke rijondersteunende functies (ADAS: Advanced Driver Assistance System) zoals Adaptive Cruise Control, Lane Departure Management Control en Intelligent Speed Adaption. ADAS gebruikt een grote hoeveelheid data uit een reeks sensoren rondom en in het voertuig om een dynamisch beeld van de omgeving op te bouwen: radar, camera, lidar, ultrageluid en GPS. Een beeld dat verder verrijkt kan worden met bijvoorbeeld rood-groencycli van kruispunten, dynamische snelheidsadviezen of informatie over wegwerkzaamheden. Omgekeerd kan uit de data die de voertuigen voor zichzelf genereren een goed beeld opgebouwd worden van de situatie op de weg, die bijvoorbeeld doorgegeven kan worden aan achteropkomend verkeer.



Automobilisten op deze wijze ondersteunen en delen van hun rijtaken overnemen, vraagt om buitengewoon betrouwbare systemen, die eenmaal in een voertuig geplaatst ook twaalf tot vijftien jaar zonder gebreken moeten blijven functioneren. Bovendien moeten ze betaalbaar zijn. De automotive-industrie zoekt dus naar manieren om nieuwe ADAS-functies betrouwbaar en kosteneffectief in te kunnen voeren. In het Europese Deserve-project (Development Platform for Safe and Efficient Drive) wordt aan een efficiënter ontwerp- en ontwikkelproces, plus een bijbehorend platform (inclusief instrumentarium) gewerkt om dit te ondersteunen. Ook wordt er gekeken naar een meer modulaire opzet van de ADAS-functies, zodat het opwaarderen of toevoegen van functies in de loop van de tijd eenvoudiger wordt. Het aandeel van toeleveranciers, voor een groot deels Nederlands, in de ontwikkeling en bouw van een auto zal naar verwachting de komende tien jaar oplopen tot zo'n 80 procent. Vernieuwers ontwikkelen oplossingen in reactie op veranderende consumentenbehoeften. Innovaties als geavanceerde sensoren en zelfrijdfuncties verbeteren niet alleen het gebruik van de auto drastisch, maar maken autodelen en proactief onderhoud ook makkelijker. Onder de vernieuwers bevinden zich NXP, TomTom, Sioux en Mind. Tesla is een belangrijke Amerikaanse voorloper. Ook internationale techbedrijven uit de IT en Telecom, als Google, Vodafone, Intel, NVIDIA en TE Connectivity zijn de arena van de auto-industrie ingestapt.

2.3 Nederland en ITS

Nederland neemt een koploper positie in met ITS (Intelligente Transport Systeem). ITS is een internationaal verzamelbegrip voor de toepassing van informatie- en communicatietechnologieën in voertuigen en transportinfrastructuur om het verkeer veiliger, efficiënter, betrouwbaarder en milieuvriendelijker te maken. Wereldwijd groeit het gebruik van ITS om regelgeving van de overheid doelmatiger te handhaven, veiligheid te bevorderen, maar ook om reizigers te informeren, te sturen en te beprijzen.

Nederland maakt zich klaar voor dit verkeersmanagement van de toekomst, waarin voertuigen zijn verbonden met elkaar en met de systemen langs de weg. Het nationaal actieprogramma Connecting Mobility geeft uitvoering aan de routekaart ‘Beter geïnformeerd op weg’. Het programma bundelt de krachten van overheid, kennisinstellingen en marktpartijen om innovaties op het gebied van Intelligente Transport Systemen te stimuleren en toe te passen. Bij coöperatieve ITS wordt data van ADAS functionaliteit Car2car en Car2Infrastructure doorgegeven. Dit werkt met een eigen wifinetwerk en in de toekomst via een 5G netwerk voor de hoeveelheid data die real time met andere auto’s en de omliggende infrastructuur gedeeld wordt. Weggebruikers raken nu al steeds meer vertrouwd met ADAS functies en kunnen met C-ITS snel inspelen op beginnende files, remmende voertuigen, incidenten, stoplichten etc. Het is belangrijk dat auto’s kunnen verifiëren dat berichten daadwerkelijk afkomstig zijn van de wegbeheerder of geautoriseerde serviceprovider- en andersom. Hiervoor wordt met certificaten gewerkt onder auspiciën van de RDW (voertuigen) en Rijkswaterstaat (wegkant). Ook voor handhaving is het noodzakelijk om zeker te weten dat de in de auto aanwezige computers (OBU’s) en certificaten niet worden gemanipuleerd. Momenteel wordt in Nederland en ook in Brussel nog hard gewerkt om deze vertrouwensketen te organiseren.

Tijdens het Europees voorzitterschap van Nederland, het eerste halfjaar van 2016, is ITS actief geadresseerd. Dit heeft o.a. geleid tot de Declaration of Amsterdam. Hierin verklaren de Transportministers van 28 EU-lidstaten gezamenlijk met de Europese Commissie en de industrie te werken aan regels en voorschriften die de ontwikkeling van zelfrijdende voertuigen op de weg mogelijk maken.

Het aantal voertuigen dat op enigerlei wijze connected is, groeit hard. Vanuit het ministerie van I&M, project Beter Benutten, worden allerlei initiatieven ontplooid en gestimuleerd om dit te bespoedigen. De komende jaren zullen staan in het teken van een afnemend niet-connected rijdend park van nu ca. 7.5 miljoen voertuigen, die zo mogelijk met een blackbox of smartphone connected worden en een groeiend aantal nieuw geleverde connected voertuigen. Ook de EU verplichte invoering van eCall functionaliteit bij nieuwe voertuigen in april 2018 zal het aantal connected voertuigen aanzienlijk doen stijgen. Autofabrikanten bereiden zich momenteel voor om dit moment te benutten voor het connected maken van hun auto’s voor bredere toepassingen dan eCall.

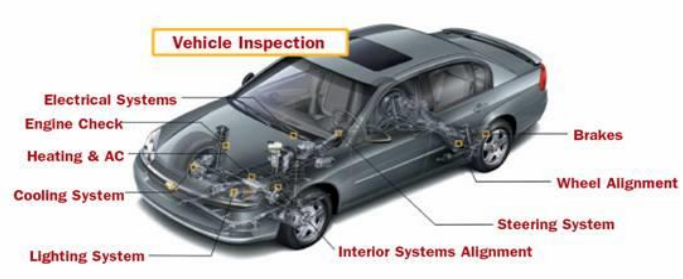
2.4 Nieuwe dienstverleners

Met data uit voertuigen zijn een heleboel services met bijbehorende verdienmodellen te bedenken. Aanbieders van deze diensten komen veelal niet uit de automotive, maar uit de wereld van de telecom, IT en techbedrijven. De auto verandert van een stuk hardware naar een rijdende computer die ook een mobiliteitsdienst verleent.

3. DATA UIT VOERTUIGEN

3.1 Periodiek en realtime

In de meeste moderne auto's zit een boordcomputer. Deze slaat allerlei gebruiksdata op via zo'n 200 sensoren in het voertuig. Een voertuig dat connected is, stuurt data naar de autofabrikant. De fabrikant kan hiermee kennis opbouwen om de auto's nog veiliger te maken en betere diensten te verlenen. De grote hoeveelheid data (bigdata) wordt verzameld in een database. Hierop kan met machine learning en database intelligentie belangrijke informatie gevonden worden.
Data wordt periodiek verstuurd bij bv. het uitlezen van de auto in een werkplaats. Bij connected auto's wordt realtime online data naar de OEM gestuurd. Dit geldt ook voor een achteraf ingebouwde device als een blackbox t.b.v fleetmanagement, volgsysteem of ritregistratie. De gegevens die doorgestuurd worden zijn voertuiggebonden (technische data omtrent conditie en gebruik) en deels proprietary, deels algemeen toegankelijk.



Ook persoonsgebonden gegevens worden verwerkt, of gegevens die tot een persoon herleidbaar zijn. Denk bijvoorbeeld aan locatie/tijdstip of technische voertuiggegevens in combinatie met IP adres voertuig/VIN/ kenteken/kentekenhouder en/of berijdergegevens.

3.2 Interne systemen af fabriek

Algemeen toegankelijk is data uit te lezen uit de OBDII (On Board Diagnostic) poort die gaat over voldoen aan wettelijke eisen als APK, en motor- en mengsel gerelateerde data. Hiervoor wordt contact gelegd met de CANbus zonder dat daarop geschreven hoeft te worden.
Alleen door de beschermde omgeving van de merkorganisatie is proprietary data uit te lezen uit de OBDII poort, waarbij ook geschreven kan worden op de CANbus. Hiermee is een grote hoeveelheid data beschikbaar over conditie/gebruik van het voertuig voor de OEM. Om reversed engineering niet te stimuleren maken OEM's het format van elk model/uitvoering en bouwjaar verschillend.

3.3 Floating Car Data

Het aantal auto's met een GPS-ontvanger aan boord groeit snel. GPS wordt voornamelijk gebruikt voor routenavigatie, maar kan ook worden ingezet voor verkeersmonitoring. Bij Floating Car Data via GPS stuurt de GPS-ontvanger via satelliet gemeten locatiebepaling door naar de centrale. Daar wordt deze data gekoppeld aan een digitale kaart en kan de vertaalslag gemaakt worden naar weggebonden verkeersinformatie. Op basis van deze informatie kunnen trajectreistijden en trajectsnelheden worden bepaald. Ook kan inzicht gekregen worden in de herkomst-bestemmingsrelatie en kan een inschatting gemaakt worden van de intensiteiten. Aan Galileo, het nieuwe en nauwkeuriger Europese GPS systeem, wordt hard gewerkt.

3.4 Externe systemen van aftermarket

Achteraf gemonteerde devices die stand alone of gekoppeld worden aan de OBDII stekker van een voertuig verzamelen voertuigspecifieke data van de CANbus en mogelijk ook data van de houder/berijder (bijvoorbeeld blackboxen of dongels). Via een SIM-kaart wordt alle data realtime doorgestuurd naar het online telematicaplatform, beter bekend als 'de cloud'. Afhankelijk van de afspraken met de opdrachtgever, bijvoorbeeld een leasebedrijf, komt de data vervolgens terecht bij de aanbieder van de device of de service-provider of het merk etc. Hier wordt alle data verwerkt zodat deze gebruikt kan worden bij de verschillende tools en rapportages. Met behulp van de 'reversed engineering' techniek worden door deviceleveranciers databases gebouwd die de proprietary data van de OEM's nabootsen.

3.5 Mobiele devices

Mobiele devices als een smartphone of tablet kunnen data via o.a. een app van het automerk versturen. Deze app zorgt voor verbinding met het voertuigsysteem. Ook standalone door de gebruiker geïnstalleerde apps als b.v. Flitsmeister of ZOOF genereren dataverkeer. Er is een groeiend aantal toepassingen in de aftermarket die op smartphones verkrijgbaar zijn.

4. DE KWETSBAARHEDEN VAN CONNECTED VOERTUIGEN

There are only two types of cars. Those that have been hacked and those that will be.

Bron: sbdautomotive.com

4.1 Complexe computers op wielen

Auto's van vandaag hebben zich dus ontwikkeld tot zeer complexe computers op wielen, met veel gespecialiseerde bedrijven die de hightech componenten en software leveren. Deze verhoogde connectiviteit brengt een aantal reële cybersecurity risico's met zich mee. De belangrijkste daarvan is de veiligheid van het voertuig. In tegenstelling tot de meeste consumentenproducten kan een inbreuk op een auto levensbedreigend zijn, vooral als het voertuig rijdt en een externe krijgt controle over de auto.

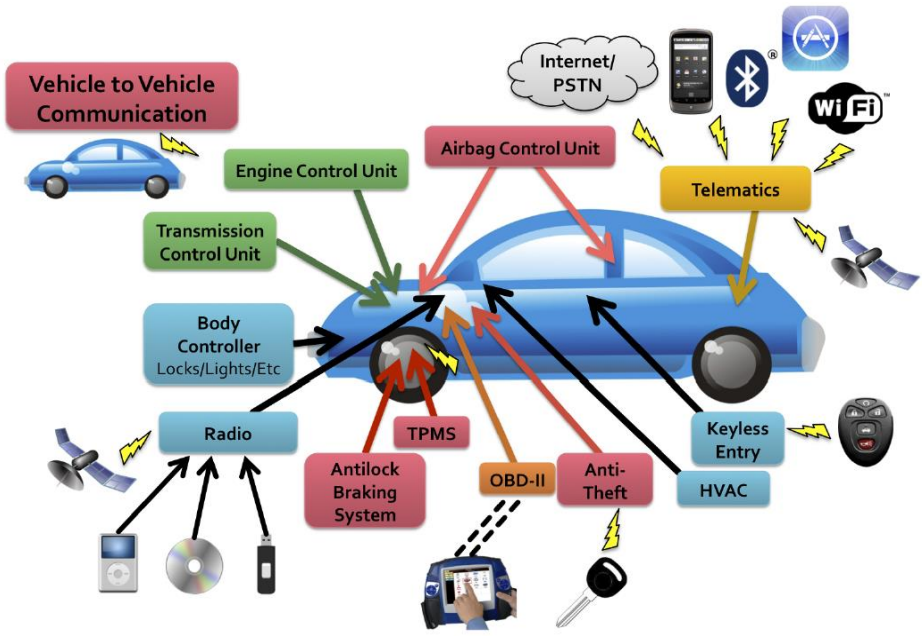
Met zo'n 30 tot 100 computers in een auto en een CANbus ontwerp uit de jaren 80 is de systeemintegratie in een auto niet optimaal. Via de OBDII poort kunnen externe systemen voor navigatie, verkeersinformatie, entertainment en handsfree functies aangesloten zijn. Denk hierbij aan een op afstand bedienbare sleutel, een radio die harder gaat als je harder rijdt, gebruik van spotify, softwareupdate van je navigatiesystem etc. Voor al deze functies wordt gewerkt met een bluetooth of internet verbinding via een ingebouwd wifi access point. Helaas is de authenticatie hierbij veelal onvoldoende. De wireless interface en de Telematica Control Units/blackbox van de aftermarket (die ook kunnen schrijven op de CANbus) worden als de zwakste schakels in de security keten gevonden. Waar autofabrikanten eerst vertrouwden op de fysieke bescherming van de auto volgens het 'kokosnootmodel' worden ze nu geconfronteerd met een bedreigende buitenwereld via de OBDII poort.

Daarom wordt momenteel bij de autofabrikanten hard gewerkt aan een compleet nieuwe IT-architectuur in de auto om de veiligheid te kunnen blijven garanderen. Tot de tijd dat deze auto's van de band rollen, zal er rekening moeten worden gehouden met auto's die op korte en lange afstand relatief eenvoudig te hacken zijn. Dit geldt zowel voor de car to car communicatie, als voor de car to infrastructure (ITS) communicatie, als voor car to smartphone (deelgebruik) en car to grid (opladen). Dit vormt een mogelijke bedreiging voor het succes van C-ITS projecten. De landelijke Smart Mobility Round Table Security heeft het dus hoog op de agenda staan en voert experimenten uit.
Met de toename van het aantal connected auto's worden deze een interessant object voor enerzijds gelegenheidscriminelen, zoals jeugd uit Westerse landen die wat rondsnuffelt op YouTube filmpjes met instructies om voertuigen te hacken. Anderzijds wordt de interesse gewekt voor georganiseerde cybercrime met een winstdoel of terroristisch doel. Dit zijn professionele 'bedrijven' vanuit de hele wereld, die goed gepland vanuit een lange termijn visie inbreken op vitale systemen.
De risico's kunnen letterlijk levensbedreigend zijn, anders dan cybercrime bij smartphones of tablets, en groots en divers. De data van en naar het voertuig om bv. te navigeren kan gemanipuleerd worden, de besturing kan beïnvloed worden voor bijvoorbeeld diefstal, data kan afgeluisterd of gestolen worden wat weer privacy en ransomware vragen oproept, software-updates kunnen ook onbetrouwbaar en ongeauthoriseerd zijn etc. De hack biedt dus de mogelijkheid om de besturing van een voertuig of een reeks van voertuigen, gepland en goed voorbereid, op afstand over te nemen. Dit biedt ook de mogelijkheid om een terroristische aanval te doen op de infrastructuur waar de voertuigen mee communiceren. Op de zwarte markt zijn tools voorhanden om m.b.v. reversed engineering de computercodes vanuit het voertuig te kunnen vertalen naar bruikbare codes voor diensten in de aftermarket. Dit roept om preventieve maatregelen.

4.2 Voertuigcriminaliteit

De datastroom naar de fabrikant wordt steeds groter, de datastromen uit andere devices nemen steeds meer toe en daarmee wordt het risico op hacken groter. Dit werkt autodiefstal en verstoring van veiligheidsfuncties in de hand.

Hackers zijn in staat om direct aan te sluiten op voertuigen en computersystemen, commando's naar verschillende on board computersystemen te sturen en daarmee controle van de motor, remmen, stuurinrichting en andere kritische onderdelen van het voertuig over te nemen. Het toenemende gebruik van navigatiesystemen (GPS, Navsat) of andere technieken die kunnen worden gebruikt om de locatie of het rijgedrag van de gebruikers te registreren, biedt zowel kansen voor opsporing als bedreigingen. Bij een aantal services is gebleken dat de inning van een breed scala van gebruikersgegevens niet alleen is om prestaties van het voertuig te verbeteren, maar ook potentieel voor commerciële toepassingen en wetshandhaving. De juistheid van deze data en de beschikbaarheid maken het eveneens belangrijk om de veiligheid te bevorderen als een integraal onderdeel van het ontwerp van het systeem (bijvoorbeeld security by design) en de noodzaak om de privacy goed te regelen bij (semi) autonome voertuigen in coöperatieve ITS. Overigens zijn ook fleetmanagers veelal in staat om de auto die connected is op afstand stil te zetten.

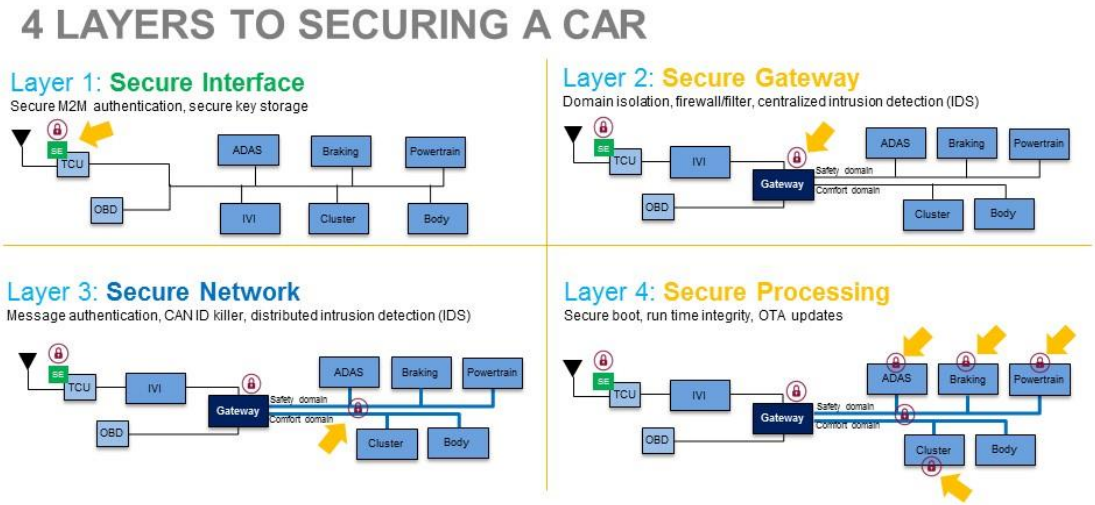


Bron: Autosec; Toenemende communicatie met omgeving zorgt voor een groter aanvalsoppervlak voor cybercriminelen.

Om risico's op een ongewenste cyberaanval te verkleinen, richten anti-virusmakers hun inspanningen op het beschermen van het vervoermiddel door betere beveiliging. Het is de bedoeling dat de beveiliging al tijdens het ontwerp wordt bedacht en tijdens de bouw van de auto wordt geïnstalleerd. Daarmee wordt het een integraal onderdeel van de hele auto-elektronica. Tot die tijd zijn er echter tal van mogelijkheden om in een auto te komen.

4.3 Activiteiten voor de toekomst

De huidige werkelijkheid is dat White hat hackers de kwetsbaarheden van connected auto's onder de aandacht brengen. Hiermee willen ze o.a. autofabrikanten, onderdelenleveranciers en aanbieders van diensten stimuleren meer aandacht te geven aan security en tevens budget vrij te maken om een lange termijn visie te ontwikkelen. Een voorbeeld van onze Nederlandse NXP, die als wereldmarktleider vele chips in de auto's levert:



Een visie waarin ook autonoom rijdende voertuigen cybersecure zijn ontwikkeld. Als straks de auto autonoom rijdt, zullen zogenaamde failsafesystemen geïmplementeerd dienen te zijn. Failsafesystemen die tijdens het gebruik kunnen signaleren dat er iets niet klopt aan het voertuig en vragen om het stuur over te nemen of het voertuig zelf richting de vluchtstrook laten gaan en tot stilstand laten komen. Ook voor wegbeheerders liggen er toekomstige rollen; zij zullen procedures voor omgaan met failsafesystemen kunnen maken en toelatingsinstanties zullen penetratietesten (hoe diep kom je in het voertuig met een hackmogelijkheid) in hun assortiment kunnen opnemen. Digitale kaartmakers zouden in de toekomst wel eens een centrale rol kunnen spelen in de security van het dataverkeer. Zij genereren big data uit Floating Car Data, wellicht zijn hier patronen in te ontdekken bijvoorbeeld op merk niveau of per land. De complexe markt van de automotive kent steeds meer stakeholders. In deze markt zijn fabrikanten gewend de lead te hebben. Maar de marktontwikkelingen gaan harder dan ze gewend zijn, met nieuwe technologieën, partijen en businessmodellen. Dit vraagt om een bredere security dan alleen het voertuig, dit vraagt om een integrale supply chain risk management aanpak, zoals de inzet van technieken die hackpogingen geautomatiseerd detecteren, de zogenaamde intrusion detection systems en analyserend forensisch onderzoek.

Op dit moment zal de vinger aan de pols gehouden moeten worden om tijdig te kunnen reageren op het moment dat cybercriminelen handel zien in het hacken van connected cars. Wie zijn de actoren, welk doel hebben ze en wanneer is er actie nodig.

4.4 Geen privacy zonder security

KPMG deed recent een consumentenonderzoek waaruit blijkt dat ongeveer de helft van de Amerikaanse consumenten bezorgd is over cyberveiligheid als het gaat om hun auto's. Naast veiligheid bevatten deze connected auto's persoonlijke informatie van apps en entertainment, locatie en persoonlijke financiële gegevens. Dit kan potentieel tot enorme schade leiden voor merken en hun verkoop. Het aanpakken van cybersecurity zou ook vanuit privacy oogpunt een hoge prioriteit voor automakers moeten hebben. De realiteit is echter dat de autofabrikanten vooralsnog de kaarten voor de borst houden. Ze geven weinig openheid over hun aanpak. Dit lijkt ook in hun saleskanaal zo te zijn: importeurs weten dat de veiligheid van het voertuig uitstekend is geregeld en beperken de kennis van connectiviteit gerelateerde functies van een gemiddelde autoverkoper tot merkgerelateerde diensten. Hierdoor blijven autokopers/consumenten onwetend. Als er data uit een auto blijkt te zijn gehackt, blijken de gevolgen voor de merkbeleving van de bestuurder echter zeer groot.

Zowel in de Nederlandse politiek als in die in Europa wordt er veel waarde gehecht aan de privacy van data van de burgers in hun dagelijkse leven in de digitale samenleving. Om de privacy van de consument en dus de security te beschermen zijn er nationaal en internationaal (nieuwe) wetten, waaronder de Nederlandse Telecomwetgeving en de Europese General Data Protection Regulation (GDPR). Deze laatste wet gaat in de basis over de bescherming van unieke data van individuen door hen controle te geven over hun eigen persoonlijke data. De GDPR gaat van kracht in mei 2018. Daarop vooruitlopend kent Nederland sinds dit jaar de Meldplicht Datalekken van de Wet Bescherming Persoonsgegevens. Data die gestolen of vernietigd is, al dan niet door hacking bijvoorbeeld uit een voertuig, dient binnen 72 uur gemeld te worden bij de Autoriteit Persoonsgegevens. Door snel en adequaat handelen van een securityspecialist kan de schade beperkt worden. Daarnaast zijn in diverse allianties van autofabrikanten passende maatregelen afgesproken om data uit voertuigen te beschermen tegen diefstal en ongeautoriseerde toegang en -gebruik. Vaak wordt vergeten om ook de gebruiker van het voertuig als een potentieel gevaar te benoemen. Hij kan door zijn al dan niet bewuste incorrecte gedrag tevens een risicofactor zijn voor cybercrime. Onder andere het via internet beschikbare 'GSMA Personal Data Programme' geeft zowel consumenten als serviceproviders mogelijkheden om de optimale balans te vinden tussen gemak, security en privacy. Hierbij staat de gebruiker met zijn eigen digitale identiteit aan het roer om veilig, gemakkelijk en laagdrempelig via een veilige userinterface in het digitale ecosysteem te surfen.

5. THE INTERNET OF INSECURE THINGS

5.1 Cybercrime zonder grenzen

Om met de aanpak van voertuigcriminaliteit bij connected auto's succesvol te kunnen zijn, is het noodzakelijk een auto als een onderdeel van het wereldwijde internet te zien. Beveiligingsbedrijf McAfee en de Amerikaanse denktank Center for Strategic and International Studies berekenden dat cybercrime de wereldeconomie jaarlijks zeker 325 miljard euro kost. Het risico om gepakt te worden is relatief laag en criminelen kunnen redelijk anoniem hun gang gaan op internet. Ze maken veelal gebruik van zogenaamde botnets, die bestaan uit geïnfecteerde computers over de hele wereld waarachter ze zich kunnen verschuilen. De bedrijven wapenen zich hiertegen door inzet van contra-spionagetechnieken, maar ook door openheid te bieden bij een aanval om anderen te helpen en publiek-privaat samen te werken op internationaal niveau.

5.2 Amerika

De Online Trust Alliance, een belangengroep van IoT leveranciers, pleit voor de invoering van een privacy en trustframework voor het Internet of Things. Ze verwachten hierbij input van de industrie, fabrikanten, ontwikkelaars en winkelketens te kunnen krijgen. Voor de consument hebben ze een 'smarthomechecklist' ontwikkeld. Ook de FBI adviseert om de Universal Plug en Play functie op routers uit te schakelen, altijd te werken met de laatste software update, en als gebruiker de af fabriek instellingen van apparaten goed te bekijken, omdat soms ongevraagd een open wifi-netwerk gecreëerd wordt. Ook maakt ze speciaal voor het hacken van voertuigen een bulletin met de do's and dont's in geval van hacking, dan wel ter preventie. En het Amerikaanse zusje van de Autoriteit Consument en Markt, de Federal Trade Commission, opende in 2015 een apart kantoor voor IoT. Zij willen de belangen van consumenten bij technologie op een breder terrein behartigen. Het gaat dan o.a. om databeveiliging, privacy, connected cars, smart homes, nieuwe betaaltechnologieën, big data en IoT.

5.3 Europa

De Europese Commissie heeft in juni 2016 een belangrijke eerste stap gezet: er is een nieuwe richtlijn goedgekeurd die handelt over de veiligheid van netwerken en informatiesystemen in de Europese Unie (de 'NIS-richtlijn'), met als doel deze beter te beveiligen.

Gezien de verontrustend snelle groei, zowel in aantallen en in sofisticatie, van cybercriminaliteit en cyberspionage is dit een belangrijke stap op weg naar een meer gecoördineerde aanpak in cyberbeveiliging in heel Europa.
De NIS-richtlijn streeft naar het verhogen van de cyberveiligheid in de EU door te zorgen voor meer paraatheid, onder andere door de oprichting van nationale CSIRT Teams (Computer Security Incident Response Teams) en een bevoegde nationale NIS-autoriteit en meer samenwerking tussen alle lidstaten, door het opzetten van de EU Coördinatie Groep. En ten slotte meer veiligheid in alle economische vitale sectoren, zoals energie, transport, water, het bankwezen, de financiële markten, (digitale) infrastructuur en de gezondheidszorg. Bedrijven in deze sectoren moeten passende veiligheidsmaatregelen nemen en ernstige incidenten melden aan de nationale autoriteit. Ook partijen met een sleutelrol, zoals digitale serviceproviders (zoekmachines, Cloud Computing diensten en online marktplaatsen) zullen moeten gaan voldoen aan de eisen van de nieuwe richtlijn.

5.4 Nederland

Nederland staat in de top 10 van landen ter wereld met de meeste cyberaanvallen. De uitstekende infrastructuur van snel, goedkoop en stabiel internet in Nederland trekt wereldwijd cybercriminelen aan, die de servers in ons land gebruiken voor hun illegale praktijken. Sinds 2012 bestaat het Nationaal Cyber Security Centrum (NCSC) als onderdeel van het ministerie van Veiligheid en Justitie. Het NCSC hecht veel waarde aan publiek private samenwerking, om gezamenlijk de weerbaarheid van de Nederlandse samenleving in het digitale domein te vergroten door tactische en operationele kennis bij elkaar te brengen en te delen. Zo kan meer inzicht worden verkregen over ontwikkelingen, dreigingen, trends en kan er meer ondersteuning worden geboden op het vlak van digitale veiligheid. Het NCSC wil daarmee een veilige, open en stabiele informatiesamenleving creëren. De afgelopen 12 maanden zijn er 400 hulpvragen naar aanleiding van een cyberaanval binnengekomen. Over de landsgrenzen heen werkt NCSC samen met de Computer Emergency Respons Teams. Verder zijn er o.a. No More Ransom, waar de Nederlandse politie samenwerkt met Europol en twee securitybedrijven. En sinds 2015 bestaat Interpol Global Complex for Innovation in Singapore, zij coördineert de wereldwijde samenwerking met technische bedrijven om cybercrime te bestrijden. Tenslotte is er The Hague Security Delta in Den Haag, dat pretendeert het grootste security cluster in Europa te zijn.

6. VERANDERENDE WERELD VAN DE AVc DEELNEMERS

Bovengenoemde ontwikkelingen raken ook de deelnemers van AVc.

6.1 Nationale politie

Sinds de herindeling van de politie bestaat het korps uit tien Regionale Eenheden en de Landelijke Eenheid. De Landelijke Eenheid bestaat uit specialistische divisies voor de bestrijding van zware, georganiseerde misdaad, infiltratie, cybercrime en anti-terreur activiteiten. De Nederlandse politie bereidt zich voor op cybercrimebestrijding. Dit lijkt niet zonder horten of stoten te gaan, aldus het beeld dat Hoofd Landelijke Eenheid in een interview in Het Financiële Dagblad schetst: Het lijkt een grote strijd om voldoende middelen binnen te krijgen en voldoende cyberspecialisten te rekruteren om cybercrime goed aan te pakken. Hij spreekt over een noodzakelijke grote herorganisatie binnen de Nationale Politie om in te springen op de toename van cybercrime in Nederland. Bovendien dringt hij aan op meer bevoegdheden bij het bestrijden van cybercrime, zoals het binnendringen van computers. Onlangs publiceerde voormalig minister Opstelten van Veiligheid en Justitie het rapport Cybersecuritybeeld Nederland, waarin de digitale weerbaarheid van Nederland wordt geëvalueerd. Volgens Opstelten blijft het de komende jaren noodzakelijk om te investeren in cybercrime.
De politie heeft een LITA (Landelijk Innovatieteam Automotive) dat onderzoeken doet op het gebied van connected cars om tactieken en technieken te ontwikkelen. Recent is gestart met het analyseren van data uit de zogeheten EDR (Event Data Recorder), die in nieuwere voertuigen is ingebouwd. Na een succesvolle proef in Rotterdam gaan 7 van de 10 politieregio's nog dit jaar van start met de EDR-uitleesapparatuur om de eventuele schuldvraag bij ongevallen beter vast te kunnen stellen.

De EDR, vergelijkbaar met de zwarte doos in een vliegtuig, registreert onder meer tijd, locatie, remgedrag, snelheid, stand van de pedalen en werking van de airbags. Bij ernstige ongevallen, waarbij de afdeling Verkeers Ongevallen Analyse van de politie onderzoek doet, kunnen de laatste vijf seconden voor het ongeluk in de EDR uitgelezen worden.
Naar verwachting draagt dit succes bij aan een prominente plaats van voertuigdiefstal en cybercrime bij connected voertuigen op de agenda van de politie. Ook andere ontwikkelingen als de oprichting van een landelijk kennis- en leercentrum voor o.a. automotive helpen om aan kennisdeling en -borging te doen. Daarnaast bestaat bij de politie de wens om een ‘kwaliteitskring’ te vormen, waarin de industrie en de opsporing verbinding kunnen vinden.
CARPOL is het EU-netwerk van politie coördinatoren voor de aanpak van voertuigcriminaliteit. Vanuit CARPOL is recent het initiatief gekomen om op Europees niveau een platform van relevante brancheverenigingen te creëren rondom het thema ‘voertuigcriminaliteit’. CARPOL verwacht een veelbelovend perspectief voor ketenaanpak van de nieuwe Europol Regulation die per mei 2017 ingaat. Door het toegenomen dreigingsbeeld in Europa adresseert Interpol steeds meer beleidsmatige thema’s als voorwaarden om criminaliteit te verlagen en publiek-private samenwerkingen te stimuleren.

6.2 Verbond van Verzekeraars

Het Verbond van Verzekeraars oriënteert zich op de innovaties en de daarbij mogelijke businessmodellen. Volgens onderzoek van KPMG zal het aantal ongelukken in 2040 met 80% verminderen door de inzet van semi-autonome auto’s. Dit vraagt om veranderingen bij verzekeraars. Connected voertuigen maken andere businessmodellen mogelijk, bijvoorbeeld om ‘Insurance as a Service’ aan te bieden. Hierbij betaalt de gebruiker afhankelijk van zijn rijgedrag (UBI). Voertuigen dienen daarvoor een telematica unit aan boord te krijgen, waarmee zogenaamde track en trace functionaliteit gemeengoed kan worden. Ook een directe autoverzekering wordt overwogen, waarbij de schade zonder schuldvraag (vergelijk een gezondheidsverzekering) verzekerd is. Bij gedeelde mobiliteit en semi-autonome voertuigen moet de aansprakelijkheid nog uitgekristalliseerd worden. De verwachting is dat steeds meer autofabrikanten ook de verzekering zullen gaan aanbieden bij zelfrijdende voertuigen. Dit heeft ook te maken met de toename van de schadelast ten gevolge van toename van de complexiteit van de auto’s, wat weer invloed heeft op de schadesturing. Schadespecialist CED stelt in het onlangs verschenen rapport ‘Moving forward in mobility’ dat de gemiddelde schadelast de afgelopen vijf jaar is gestegen met 13%. Met de toenemende connectiviteit van auto’s zal het schadebedrag door vernuftige en meer geïntegreerde technologie steeds forser worden. Elektronica en geïntegreerde onderdelen zijn steeds meer merkspecifiek, wat repareren duurder maakt.

6.3 RDW

De RDW rondt eind 2016 het programmaplan VICTOR af. VICTOR staat voor ‘Voertuig-, Informatie Communicatie Technologie OntdekkingsReis’. VICTOR maakt een verkenning om kennis en praktijkervaring op te doen op het gebied van ITS. Hoofddoel van het programma VICTOR is een roadmap richting de toekomst op te leveren, omdat ITS-ontwikkelingen vooral ICT-gerelateerde onderwerpen zijn, die een prominente rol gaan spelen in het voertuigdomein. Het voorliggende programmaplan gaat over onderwerpen zoals ‘hoe om te gaan met dynamische voertuigdata’, ‘het nieuwe toelaten en toezicht’, ‘embedded software’, ‘sensoren’, ‘kennisopbouw’ en ‘de medewerkers van de toekomst’. Voor de RDW betekent dit mogelijk een omslag van een fysieke Europese typegoedkeuring voor toelating van voertuigen op de weg naar een continue landelijke softwarecertificering van een voertuig. Een geüpdatet auto moet immers ook na de update weer voldoen aan de eisen. Hierbij spelen ‘performance based standards’ een grote rol. Zij zijn de aangewezen partij om het configuratiebeheer van voertuigen in Nederland te beheren op VIN en/of bijvoorbeeld IP adres van de auto. Bij het ontwerpen van de infrastructuur voor dit soort configuratiebeheer wordt cybersecurity nadrukkelijk geadresseerd. De RDW zoekt hiervoor samenwerking met partijen zoals de ANWB, Beijer, andere overheden en kennisinstellingen. In het voorjaar van 2016 heeft de RDW het rapport ‘Data in a vehicle’s lifecycle’ opgeleverd. Hierin wordt naast bigdata uit voertuigen, ook kort aandacht gegeven aan vehicle crime op dit moment. Onderscheiden worden diefstal van het voertuig, de kentekenplaat, het kentekenbewijs, onderdelen of anders. De RDW staat aan de vooravond van oriëntatie op security requirements rondom connected voertuigen. Denk aan digitale aanvallen die ze doorkrijgen van het Nationaal Cyber Security Centrum, manipulatie van motormanagement systeem, datadiefstal, datamisbruik (zwartrijden) autorisatie van software-updates en betrouwbaarheid bij C-ITS toepassingen (Public Key Infrastructure). Door bovengenoemde bigdata, bestaand en nieuw, te ontsluiten en te verbinden met de business en de processen van de RDW worden nuttige kansen gecreëerd voor de uitvoering van de taken van de RDW.
Europees gezien vervult de RDW een koploper rol; men onderhoudt hiervoor contacten met UNECE en EReg t.a.v. wet- en regelgeving.

6.4 Ministerie van Veiligheid en Justitie

Momenteel is er een wetsvoorstel Computercriminaliteit III, ook wel populair de ‘terughackwet’ genoemd. In deze wet wordt het aantal digitale opsporingsmogelijkheden voor politie en Openbaar Ministerie uitgebreid om de opsporing en vervolging van (cyber) criminelen te versterken. Belangrijkste nieuwigheid in de Wet Computercriminaliteit III is dat de politie onder strikte voorwaarden zelf computers mag hacken. Tot op heden mag, zelfs als logingegevens van criminelen worden gevonden, de politie die niet gebruiken om op afstand in te loggen op computers of internetaccounts. De politie mag onder de nieuwe wetgeving ook gegevens kopiëren, aftappen (ook uit de cloud) of ontoegankelijk maken op de computer van een crimineel.

De bevoegdheden mogen echter ook worden ingezet bij andere vormen van cybercrime, zoals het gebruik van botnets om kwaadaardige software te verspreiden. Verder maakt het wetsvoorstel het een misdaad om gegevens te 'helen' die bij computerhacks zijn gestolen. Er wordt in de wet gesproken over zogenaamd ‘geautomatiseerde werken. Hieronder kunnen ook autonavigatiesystemen en auto’s gerekend worden. Hacken door de politie kan een behoorlijke privacy-inbreuk opleveren voor de eigenaar van de gehackte computer. Verschillende organisaties, waaronder de Autoriteit Persoonsgegevens en Bits of Freedom, vinden dat de wet een te grote inbreuk op de privacy betekent en dat er onvoldoende waarborgen zijn om misbruik te voorkomen. Ook willen zij onafhankelijk toezicht op de toepassing van de bevoegdheid. Tevens zijn er zorgen over het misbruik van 'achterdeurtjes' in software door de politie en de inzet van spyware. Die zou computers immers onveiliger kunnen maken, terwijl de politie juist cybercrime probeert te bestrijden. De discussie over de Wet Computercriminaliteit III vindt plaats in de aanloop naar het debat over de nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten later dit jaar, waar opnieuw veel van dezelfde vragen over de balans tussen privacy en veiligheid zullen langskomen.
Het ministerie van Veiligheid en Justitie heeft hacking en diefstal als beleidsterrein. Er lijkt echter nog geen interdepartementaal overleg met betrekking tot cybercrime in connected voertuigen te zijn met bijvoorbeeld het Ministerie van Infrastructuur en Milieu.

6.5 BOVAG en RAI Vereniging

Zowel BOVAG als RAI Vereniging staat aan de vooravond van oriëntatie op security aspecten bij connected voertuigen en wat dat voor leden kan betekenen. Op dit moment zijn ze beland in de discussie over data uit voertuigen en wie daar zeggenschap over heeft. Daar waar het connected voertuig veelal de data naar de autofabrikant zendt, lijkt ook de aftermarket toegang tot die data te willen om ‘op maat’ mobiliteitsdiensten te kunnen ontwikkelen. De brancheorganisaties zetten daarom in op bewustwording en standpunt bepaling voor hun leden. Daarnaast lijken importeurs en dealers door de autofabrikanten nog weinig geïnformeerd te worden over de connectiviteit van voertuigen, anders dan noodzakelijk om connectiviteitsdiensten als merk gelieerde service te verkopen. Dit vertaalt zich ook terug in de showroom; kennis van rij ondersteunende functies en connectiviteitsfuncties behoeft nog meer aandacht. Volgens onderzoek van VWE heeft op dit moment ca. 20% van de nieuw verkochte auto’s ADAS functies. Een goede voorlichting bij consumenten zou de security ten goede kunnen komen.

6.6 ANWB

ANWB lijkt zich (inter-)nationaal goed voor te bereiden op haar belangenbehartigingsrol en haar commerciële kansen bij connected voertuigen voor de leden. Via de FIA is de ANWB op Europees niveau actief in o.a. hun pleidooi voor Europese regelgeving over de zeggenschap over data. Daarnaast zijn zij een onderdeel geworden van een internationale telematica alliantie (INTelematics) samen met Australische, Britse en Oostenrijkse zusterondernemingen. Dit heeft als doel om kennis te delen, producten te ontwikkelen en de samenwerking aan te gaan met autofabrikanten. In Nederland testen ze sinds twee jaar met zo'n 1000 dongels in voertuigen als basis voor een verkeersveilige autoverzekering. Tevens voeren ze bigdata analyse uit op binnengekomen data/informatie om de Wegenwacht auto vooraf te kunnen informeren waar hij nodig is en wanneer. Ook bieden ze blackboxtechnologie als ledenproduct aan. Het lijkt erop dat ANWB zich met deze ervaringen o.a. klaarstoomt voor een rol bij de invoering van eCall in april 2018. Dit om als Third Party Service hulp te kunnen verlenen bij een emergency call. Hiervoor hebben ze toestemming nodig van de berijder van het voertuig om de auto te tracken. Hoe meer leden vertrouwd zijn met connected zijn met de ANWB, hoe meer diensten verleend kunnen worden. Ondanks dat ze zelf zeggen 'many questions, few answers' staat security in bovengenoemde ervaringen hoog op de agenda.

6.7 TLN

Gezien de scope van het onderzoek is in dit kader niet direct met TLN gesproken. De transportsector kent meerdere beweegredenen, financiële en logistieke, om connectiviteit in de vloot in te voeren. Ze zijn er dan ook eerder mee gestart en hebben succesvolle pilots, mede op het vlak van aanpak van voertuigcriminaliteit, op hun naam staan. De hiermee opgedane ervaring kan door de overige partners binnen AVc zeker worden benut.

6.8 ARN

De veranderende mobiliteit vraagt om een kortere time to market van auto's en leidt tot een kortere levensduur van intensiever gebruikte deelauto's. Deze optelsom vereist een radicale innovatie van auto-ontwerp en materiaalgebruik, waardoor circulariteit in de auto-industrie prioriteit moet worden. Ondertussen is ook de tweedehandsmarkt voor voertuigen aan het veranderen.

Composieten en geavanceerde elektronica in auto's zijn in opkomst. Demontagebedrijven vrezen dat ze in de toekomst niet de technologische kennis zullen hebben om te blijven recyclen zoals ze dat doen. Er zullen waarschijnlijk gespecialiseerdere dienstverlenende bedrijven komen, sommige onder het merk van de fabrikant zelf. Deze bedrijven zullen zich bezighouden met specifieke taken, zoals auto-accu's recyclen aan het einde van hun gebruikscyclus. Er is behoefte aan meer samenwerking tussen de leveranciers en de rest van de keten, van begin tot eind. ARN is daarom recent deelnemer van de Automotive Campus in Helmond geworden. ARN verleende haar medewerking aan een rapport hierover van ABN AMRO. Of ARN in de toekomst ook rijdende computers gaat slopen en hoe het dan zit met de security is nog niet gezegd.

7. CONCLUSIES & AANBEVELINGEN AAN AVc

7.1 Conclusies

Voorliggend onderzoek m.b.t. de effecten van connected personenvoertuigen op de aanpak van voertuigcriminaliteit heeft geleid tot een aantal conclusies op hoofdlijnen:

Het aantal voertuigen dat op enigerlei wijze connected is, wordt in 2020 op 75% verondersteld. Dit gebeurt door toenemende inzet van leaseauto's die af fabriek connected zijn of later voorzien worden van een zogenaamde blackbox. Ook o.a. verhuur- en deelauto's met een blackbox dragen bij aan deze groei, net zoals de C-ITS stimulerende maatregelen vanuit de overheid. Tenslotte zal de verplichte eCall functionaliteit binnen voertuigen de fabrikanten de mogelijkheid geven nieuwe voertuigen gelijktijdig voor meer toepassingen connected te maken.
Hiermee worden onder andere track- en trace mogelijkheden bij 75% van de voertuigen mogelijk.

Connected voertuigen zijn rijdende computers met een IP-adres. Zij produceren dagelijks gigabytes aan data, die o.a. naar de autofabrikanten en mobiliteitsproviders gaan. Ook toepassingen op de smartphone van de gebruiker genereren voertuig gerelateerde data en wegkantsystemen hebben ook data. Deze bigdata biedt tal van identificatiemogelijkheden van een voertuig.

Op dit moment is de zeggenschap over data voor mobiliteitsproviders, verzekeraars, consumenten, leasebedrijven en andere belanghebbenden nog volop punt van discussie. De autofabrikant gaat in toenemende mate met de consument praten. Hiermee is ook de privacy van data vanuit voertuigen een onderwerp. De auto maakt onderdeel uit van de digitalisering van de samenleving, van Internet of Things en als zodanig is deze discussie niet anders dan zoals die in Nederland en in Europa volop gevoerd wordt bij het tot stand komen van wetgeving (GDPR) rondom consumentenprivacy.

Deze digitalisering brengt ook bedreigingen met zich mee. De veiligheid van voertuigen staat voor fabrikanten hoog in het vaandel. Echter de veiligheid van het voertuig connected met bijvoorbeeld wifi-technologie, softwaredownloads uit de cloud of OBDII koppelingen vanuit de aftermarket staat onder druk.

Cybersecurity verdient aandacht. Temeer omdat Nederland, als hoog gedigitaliseerd land, de vijfde plaats inneemt op de wereldranglijst van aantal cybercrime delicten. Veelbelovende wetgeving, als de Criminaliteitswet III, is hiervoor in de maak. Cybercrime stopt niet bij de grens en dus heeft ook de Europese Commissie de NIS richtlijn omarmd.

Voor de Stichting AVc en haar deelnemers biedt dit nieuwe uitdagingen. Deelnemers geven allen vanuit hun eigen perspectief reeds aandacht aan diverse ontwikkelingen. Er verschijnen bovendien nieuwe partijen bij de innovatie van voertuigen en dienstverlening rondom voertuigen, die een schakel kunnen zijn bij de publiek-private samenwerking in de aanpak van voertuigcriminaliteit.

Het bewustzijn van de consument rondom cyberrisico's is nog niet groot. Toch moeten consumenten er blijvend op kunnen vertrouwen dat hun auto veilig is. Op basis van de huidige hackactiviteiten blijkt dat de security van connected voertuigen nog onvoldoende is. Hiermee kan het een potentiele bedreiging voor de ontwikkeling van connected voertuigen zijn. Immers, niemand wil op de snelweg stilgezet kunnen worden door cybercriminelen. Desondanks is de aandacht voor security bij de autofabrikanten, toeleveranciers en dienstverleners nog weinig zichtbaar. Ook in de transitie fase naar autonoom rijden is dit een item.

Het borgen van security vormt een onderdeel van de gehele levenscyclus van een voertuig. De zwakste schakel is ook hier bepalend voor de kracht van de hele keten. Daarom is een 'end to end' aanpak gewenst. Het helpt niet als de voordeur goed beveiligd is, maar de zijdeuren nog openstaan. Internationale samenwerking is belangrijk, want cybercriminelen gebruiken vaak netwerken met infrastructuren verspreid over de hele wereld. Security is te lang genegeerd. Het dient hoger op de agenda te komen staan. Hier ligt ook een rol voor de overheid. Het betreft immers safety- /security risico's die in potentie levensbedreigend zijn. Security is een voorinvestering in consumentenveiligheid en privacy.

7.2 *Aanbevelingen*

Onderstaand wordt een aantal aanbevelingen aan AVc en haar deelnemers (soms vertaald naar hele concrete producten) genoemd, die aandacht zouden kunnen krijgen in het kader van de aanpak van voertuigcriminaliteit bij connected voertuigen.

7.2.1 *Volg ontwikkelingen*

Volg de ontwikkelingen (b.v. TU Automotive Cybersecuritycongressen, The Hague Security Delta themacafés) die veelbelovend kunnen zijn voor de aanpak van voertuigcriminaliteit en deel de kennis hieromtrent.

- ✓ Breng partijen samen uit de automotive sector en stimuleer voorlichting over security uitdagingen.

- ✓ Stel zo nodig een accountmanager per AVc deelnemer aan om intensief de contacten te onderhouden en kennisdeling te kunnen organiseren/faciliteren.

Wees betrokken bij diverse ontwerpprocessen van de ontwikkelingen als C-ITS.

- ✓ Vraag tijdens de transitiefase naar C-ITS aandacht voor de kwetsbaarheden van het voertuig als onderdeel van het C-ITS secure ecosysteem. Vraag daarbij aandacht voor de inzet van een EDR (Event Data Recorder). Haak hierbij aan bij bv. het spel van het ministerie van I&M, SimSmartMobility.

7.2.2 Werk aan bewustzijn

Vraag daarbij aandacht voor zaken als standaardisering en certificering.

- ✓ Vraag aandacht voor uitbreidingen van het RDW Register met o.a. IP adres van een voertuig voor bigdata forensisch onderzoek.

- ✓ Stimuleer certificering die kijkt naar het apparaat in zijn ecosysteem en die beter aansluit op ontwikkelingen van het voertuig. Stimuleer de certificering van dongels en blackboxen. Stimuleer ook andere relevante keurmerken zoals Stichting Keurmerk Ritregistratiesystemen om vanuit een security oogpunt hun keurmerk te bezien.

- ✓ Vraag aandacht voor onderzoek vanuit security overwegingen naar het gebruik van smartphones voor voertuigtelematica in plaats van blackboxen en dongels.

Kijk naar de meerwaarde van de ‘levenscyclusbenadering’.

- ✓ Stimuleer een op te richten consortium voor ‘Security by design’. Leveranciers gaan intensief samenwerken en de banden aanhalen met autofabrikanten en andere spelers in de waardeketen. Vraag hierbij aandacht voor de principes van ‘security by design’.

- ✓ Maak een plan over security tijdens de levenscyclus van de auto. Gedacht kan worden aan certificering (d.m.v. een geheimhoudingsverklaring) van werknemers in de automotive die met data uit voertuigen werken. Neem bijvoorbeeld in de berijdersinstructie op dat bij inleveren van de leaseauto de persoonsgebonden data gewist is. Denk na over wat er met de blackbox gebeurt bij verkoop van een voertuig etc.

Werk aan bewustzijn van het criminaliteit-element bij de ontwikkelingen binnen de mobiliteitssector.

- ✓ Innovaties bij toeleveranciers van de automotive komen voor 55% uit Nederland. Zij zullen een steeds grotere businesspartner van de autofabrikanten worden om de innovaties en het tempo te leveren van veilige producten die de veranderende consumentenvraag aan kan. Nederlandse toeleveranciers kunnen in die hoedanigheid proactief aan security voor voertuigen werken. Bij Automotive Campus in Helmond komen veel lijnen samen. Maak hier contact mee.

Werk aan consumentenbewustzijn.

- ✓ Vlieg het aan door aandacht te vragen voor consumentenprivacy, die reeds aandacht heeft, onder het mom van ‘Geen privacy zonder security!’.

- ✓ Zorg dat ook indirect het bewustzijn van consumenten toeneemt bij het gebruik van het connected voertuig als onderdeel van Internet of Things.
  Gedacht kan worden aan een cybersecuritycijfer voor een voertuig, een smart voertuig checklist naar voorbeeld van Online Trust Alliance, een hoofdstuk ‘vermoedelijk gehackt voertuig’ in de consumentenhandleiding, een opt-out voor berijders voor datadelen, een opt-in ten behoeve van opsporing of hacking etc.

- ✓ Verken de mogelijkheden van crowded system security voor vermiste voertuigen, werkend zoals het landelijke waarschuwingssysteem AMBERalert voor vermiste kinderen functioneert. Of overweeg de verdere inzet van Meld Misdaad Anoniem in dit kader.

Breng partijen met elkaar in contact.

- ✓ De connected voertuigen en dienstaanbieders daarin en er omheen kennen vele, voor automotive, nieuwe spelers. Intensiveer de banden met andere spelers in de waardeketen. Betrek ze inhoudelijk bij stappen richting gezamenlijke ontwikkeling en cocreatie voor de aanpak van voertuigcriminaliteit. Stimuleer om zorgvuldig met certificatenuitgifte om te gaan. Prominente rollen worden verwacht van telecombedrijven als Vodafone Automotive, kaartmakers als HERE, TomTom, systemintegraters als IBM, security bedrijven als UL etc.

- ✓ Stimuleer interdepartementale ontmoetingsmomenten.
  De ontwikkelingen van coöperatief rijden (C-ITS) met connected voertuigen worden vanuit het Ministerie van Infrastructuur en Milieu flink aangejaagd. Security is een onmisbare schakel voor succesvolle C-ITS toepassingen. Een gezamenlijk dossier op dit vlak met het Ministerie van Veiligheid en Justitie lijkt dan ook zeer wenselijk.

- ✓ Zoek een quick win.
  Mobiliseer energie en organiseer een showcase of een hackathon met blackboxen van de aftermarket om aandacht voor de security uitdaging van nu te vragen. Of maak, als een echte 'white hat hacker' een video.

Betrek inhoudelijk potentiele deelnemers bij AVc.

- ✓ Er zijn diverse partijen, die qua databeschikbaarheid voor opsporing een bijzondere positie innemen: RWS als wegbeheerder, Telecombedrijven, Techbedrijven, Vereniging van Nederlandse Fleetowners (VNF), Vereniging van Nederlandse Autoleasemaatschappijen (VNA), Vereniging Zakelijke Rijders (VZR), Private onderzoekspartijen en de alarmcentrales.

Probeer te leren van ontwikkelingen elders (andere sectoren maar ook op dit domein in bijvoorbeeld de VS).

- ✓ Kijk over de schutting bij TLN, Amerika, landen waar connected voertuigen al redelijk ingevoerd zijn, zoals Engeland met blackboxen voor Usage Based Insurance.

7.2.3 Versterk publiek-private opsporing

Zet in op een versterking/ontwikkeling van publiek-private opsporing. Connected voertuigen zijn immers beter traceerbaar en deze kans kan optimaal worden benut.

- ✓ Autobezit verschuift meer en meer van consumenten naar fabrikanten, leasebedrijven en dienstverleners. De auto's hebben de laatste technische mogelijkheden van traceren. Opsporing lijkt met de toename van dergelijke en merkconnected voertuigen en eCall eenvoudiger te worden. Publiek-private samenwerking is dan evident. Werk aan een stelsel van afspraken (PPS) voor opsporing via eCall/GSM.

Verschuiving opsporing van publiek naar privaat.

- ✓ Er worden vanuit het publieke domein steeds meer en in een vroeger stadium private partijen betrokken bij innovatieve opsporingsmethoden. Ook de politie maakt in toenemende mate gebruik van private opsporingsbedrijven en techbedrijven. Laat de branche voor cybersecurity en andere organisaties daarom samenwerken in de zoektocht naar manieren om terug te vechten.

- ✓ Nederland vervult voor C-ITS een unieke koploperpositie. Het zou mooi zijn om bij CARPOL de interesse te wekken voor de cybersecurity kant van C-ITS, dit aan de agenda toe te voegen en samen met Europese koploper RDW bij te dragen aan de risicoanalyse.

- ✓ Deze tijd van ongelimiteerde computercapaciteit biedt mogelijkheden voor opslag van grote hoeveelheden data waarmee door middel van Business Intelligence (Business Forensics) software patronen zijn te herkennen, crosslinks door bestanden te maken etc. Connected voertuigen genereren heel veel data vanuit diverse devices, die in het kader van preventie en opsporing nuttige informatie als patroonherkenning kunnen leveren. Intensiveer hiervoor de samenwerking met het Landelijk Informatiecentrum Voertuigcriminaliteit als operationeel en coördinerend informatieplatform in publiek private samenwerking en overweeg een pilot.

Benut hierbij ook de kansen die voortvloeien uit verscherpte wetgeving als Computercriminaliteitswet III en de Europol Regulation rondom datamisbruik/hacking.

- ✓ Cybercrime is moeilijk tegen te gaan omdat het zo'n lucratieve business is; hogere straffen maken cybercriminaliteit dan ook veel minder lonend. Vraag aandacht voor het ongebreidelde bezit en gebruik van eenvoudige tools (beschikbaar op internet) of jammers.

7.2.4 Benoem een expertgroep

En last but not least, *v*oor AVc is het belangrijk de veranderende wereld te begrijpen en de gevolgen te kunnen overzien om de aanbevelingen verder vorm te geven. Stel hiervoor een groep samen, waarin experts uit het vakgebied deelnemen en die zich bezighouden met 'what if' scenario's. Bedenk als AVc tenslotte wat de visie en missie is en welke rol AVc wil spelen in de cybersecurity van voertuigen en daaraan gelieerde criminaliteit, m.a.w. waar start en eindigt de scope. Geef aandacht aan hoe de strategie en de veranderingen binnen AVc geïmplementeerd kunnen worden.

MET DANK AAN

Marc Greven	ACEA
Remco Evers	Achmea
Andre de Boer	ALD Automotive
Ferry Smith	ANWB
Evert Jeen van der Meer	AON
Arie de Jong	ARN
Bram Hendrix	AutomotiveNL
Bas van der Zijden	BMW
Koos Burgman	BOVAG
Rene Engelen	Bovemij
Nick Juffermans	Connekt
Joelle van de Broek	DTCIM
Joost Vantomme	Febiac
Tjibbe Gaastra	HERE
Gilles Ampt	ITS Roundtable Security
Monier El Berrah	KIWA SCM
Rence Damming	KPN
Wout Benning	Mercedes Benz
Melle Vroom	Min. I & M
Maurice Geraets	NXP
Willem Lagendijk	Politie
Tjeerd Tuitel	PON/MIND
Henk Bos	RAI Vereniging
Gerben Feddes	RDW
Marcel Otto	RWS
Bert Dodde	Stichting AVc
Werner Postma	Stichting AVc
Arjan Geluk	UL
Herbert Leenstra	Universiteit Leiden
Ton Mesker	VNA
Marly de Blaeij	Verbond v. Verzekeraars

Colofon:

Uitgegeven door	Stichting Aanpak Voertuigcriminaliteit secretariaat@stavc.nl 088–5543201 www.stavc.nl
Uitgevoerd door	Bètaflow, Josée Sombekke joseesombekke@online.nl 06–40330364
Datum	December 2016