Gebrek aan cyber security bedreigt autonoom rijdende auto

Leenstra, H.; van den Berg, Jan; van Wee, Bert

Publication date
2017

Document Version
Final published version

Published in
Verkeerskunde: vaktijdschrift over verkeer en vervoer

Citation (APA)
Leenstra, H., van den Berg, J., & van Wee, B. (2017). Gebrek aan cyber security bedreigt autonoom rijdende auto. *Verkeerskunde: vaktijdschrift over verkeer en vervoer*, (1), 8-16.

Gebrek aan cyber security bedreigt autonoom rijdende auto

Drs. Herbert Leenstra, KPN, Prof. dr. ir. Jan van den Berg, TU Delft en Universiteit Leiden, Prof. dr. Bert van Wee

Connected- en de autonoom rijdende auto's communiceren constant met hun omgeving. Deze rijdende computers zijn nooit ontworpen om kwaadwillende hackers buiten te houden. Het is tijd om de ICT architectuur in onze auto's grondig te herzien om ervoor te zorgen dat de fysieke consumentenveiligheid gegarandeerd wordt. Onderzoek vanuit de Cyber Security Academy in samenwerking met Universiteit Delft en Universiteit Leiden laat zien welke stappen er genomen kunnen worden om de cyber security van personenauto's te verbeteren.

Kernwoorden: Cyber security, autonoom rijdende auto, connected car, hacking, ICT systeem veiligheid.

Volgens de 2016-cijfers van het CBS zijn er in Nederland 7 miljoen personenauto's in bezit van particulieren. Eerdere CBS cijfers laten zien dat 72 procent van de Nederlandse huishoudens een auto bezit. [1] Onderzoek door Jiang laat zien dat de trend om auto's met hun omgeving te laten communiceren binnen afzienbare tijd zal resulteren in autonoom rijdende auto's.

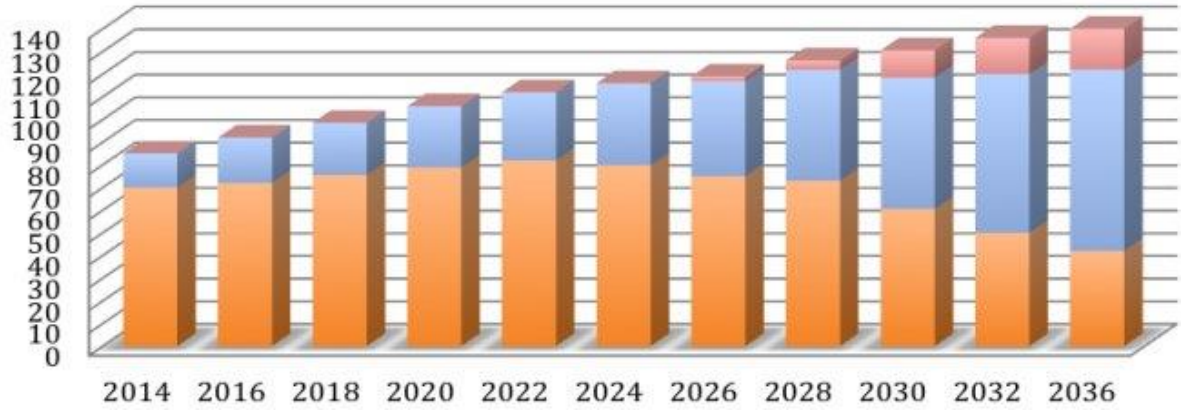

Fig. 1. Global Market for cars in mln, Traditional driven car, Semi-autonomous car, Autonomous car [2]

In de connected, of semi-autonoom rijdende, auto neemt de auto een deel van de taken van de bestuurder over. Voorbeelden hiervan zijn cruise control, en "lane assist". Onderstaande relatie diagram geeft de verhouding weer tussen de connected – en de autonoom rijdende auto weer. De trend om auto's steeds verder autonoom te maken is hoofdzakelijk ingegeven door drie factoren.

[1] CBS, Centraal Bureau voor de Statistiek, 2015 & 2016.
[2] Jiang, T., et al, 2015 p6

De eerste factor is dat 94% van alle ongelukken bestuurder gerelateerd is. [3] Bestuurders kunnen hulp van geautomatiseerde systemen gebruiken bij het schadevrij rijden. Een tweede argument is dat er door het automatiseren van auto's, minder files ontstaan en het wegdek optimaal gebruikt kan worden, wat ook het milieu ten goede komt.

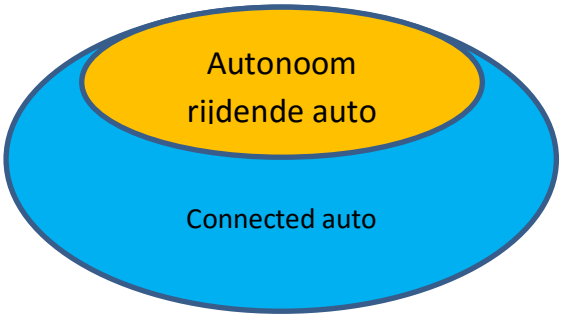

Fig 2. Relatie diagram connected – en autonoom rijdende auto

Het laatste argument is dat de bestuurder minder stress ervaart en tijd krijgt om andere zaken te doen tijdens het rijden. [4] [5] Door het koppelen van sensoren en systemen is de ICT component in de auto steeds belangrijker geworden. Een gemiddelde auto bevat 50-70 ECU's [6].(Electric Control Unit). De diverse systemen in de auto communiceren via de CAN bus. [7] Het is nu mogelijk door het hacken van de ICT systemen van de auto, ook de fysieke veiligheid van de bestuurder in gevaar te brengen.

Doel van het onderzoek is om te kijken of connected auto's cyber secure zijn en zo niet wat dan de concrete mogelijkheden zijn voor de actoren om deze cyber security te verbeteren. Uit literatuuronderzoek blijkt dat hierover nog niet veel is gepubliceerd. De onderzoeken die beschikbaar zijn gaan veelal over de technische mogelijkheden of over het profileren van hackers. Ons onderzoek is gebaseerd op literatuuronderzoek dat geverifieerd is via diverse interviews in de Nederlandse automotive sector. Zo zijn er interviews gehouden met de overheid (RDW), kennisbedrijven, verzekeringsorganisatie, brancheorganisaties, fabrikanten en diverse andere belanghebbenden in de automotive industrie. Tenslotte is er ook een enquête gehouden om ook op die wijze de gevonden resultaten te controleren. De methode en de gecombineerde resultaten van de drie bovenstaande methoden zijn gedetailleerd beschreven in het onderzoek.

Het onderzoek is opgebouwd uit drie componenten. In het eerste deel is gekeken naar de technische aanvalsvectoren die mogelijk zijn om een connected auto te compromitteren. In het tweede deel van het onderzoek is er een hacker analyse opgesteld om per type aanvaller de prikkel te identificeren om een auto aan te vallen. Door het wegnemen van deze prikkels kan een auto beter worden beschermd. In het derde deel van het onderzoek zijn de resultaten van de eerste twee delen

[3] Singh, S., 2015
[4] Heide, A. et al., 2006
[5] Volvo, 2016b
[6] ECU, Electronic Control Unit
[7] CAN, Controller Area Network. Een bus netwerk in de auto dat verschillende systemen koppelt.

gecombineerd en zijn er concrete stappen gedefinieerd die de automotive sector kan nemen om auto's cyber secure te maken.

Zoals het schema hieronder laat zien zijn er veel aanvalsvectoren mogelijk om een auto aan te vallen. Nu de huidige generatie auto's verbonden is met het internet, kunnen hackers ook via het internet auto's hacken. [8]

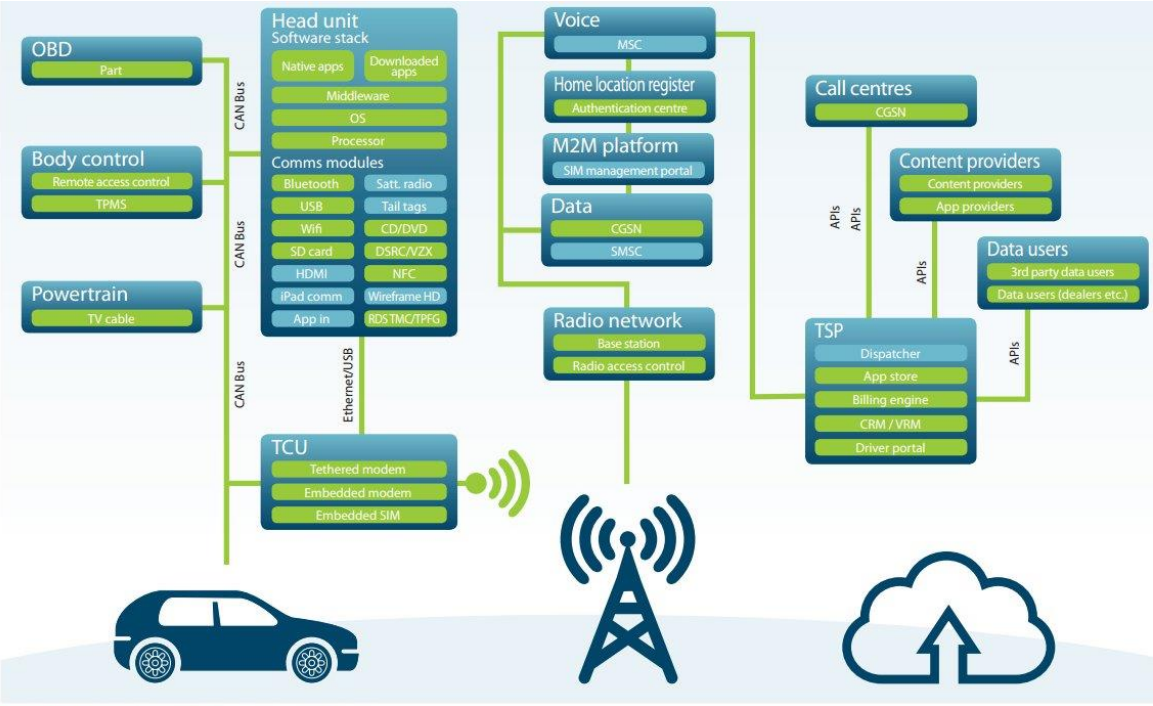

Fig. 3. Gedetailleerd overzicht van mogelijke aanvalsvectoren van een connected auto. [9]

Als we de mogelijke aanvalsvectoren clusteren ontstaan er vier categorieën. Het eerste aanvalscluster bestaat uit directe fysieke toegang. Als mensen directe fysieke toegang hebben tot de auto, kan men de software van de auto manipuleren. Dit kan bijvoorbeeld door gebruik te maken van de OBDII poort tijdens een onderhoudsbeurt of tijdens het repareren van een auto. Het tweede cluster bestaat uit de indirecte fysieke aanval. Hiervoor heeft de aanvaller een drager nodig om in de ICT systemen van de auto te komen. Denk bijvoorbeeld aan een USB stick met een firmware update voor de auto [10] of een muziek CD die malware bevat. Het derde cluster bestaat uit draadloze aanvallen via bluetooth, WiFi of mobiele telefoon. In de

[8] Smith, C. 2016; Checkoway, S et al., 2011; Valasek, C; Miller, C., 2013

[9] TU Automotive, 2016

[10] Fiat Chrysler Automobiles (FCA) 2016 https://www.fcagroup.com/en-US/Pages/home.aspx is een groot automobiel consortium. Merken die onder de FCA groep vallen zijn: Abarth, Alfa Romeo, Chrysler, Dodge, Fiat, Jeep, Lancia, Ram, SRT en Maserati. De update site voor de FCA "Uconnect service" is http://www.driveuconnect.com/software-update/ De eindgebruiker kan hier de software update downloaden voor zijn auto. De software download is gebaseerd op het VIN, Vehicle Identification Number. De software download kan op een USB stick gezet worden waarna de eindgebruiker zelf zijn auto software kan bijwerken. Het duurt 30 tot 45 minuten om de software van de auto bij te werken.

afgelopen periode zijn diverse voorbeelden in de media gepubliceerd waarbij auto's via deze weg werden gehackt. Via de genoemde drie categorieën kan een hacker de software manipuleren en de configuratie instellingen van de auto wijzigen. Dat is niet mogelijk met de vierde en laatste categorie. De laatste categorie bestaat uit het misleiden van de sensoren met valse informatie. Zo kan men een Lidar [11] sensor laten denken dat er een object op de weg staat zodat de auto plotseling remt.

Er bestaat niet één soort hacker. Er zijn diverse soorten hackers die elk hun eigen incentives hebben. In de hacker analyse is gebruik gemaakt van het SABSA-framework.[12]

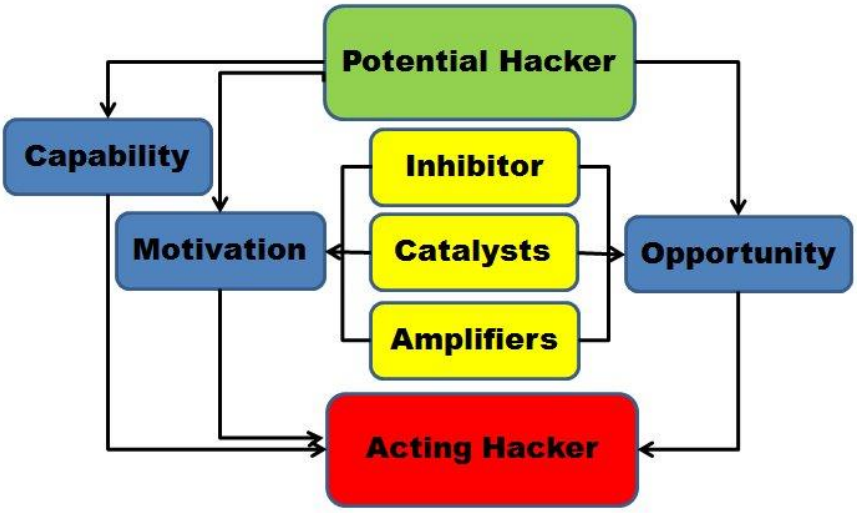

Fig 4 SABSA framework, actor elementen, Sherwood.

De technische opportunity factor is hierboven beschreven in de technische aanvalsvectoren. Literatuur over de motivatie factor van hackers geeft aan dat de motivatie factoren terug te brengen zijn tot: geld, kennis, macht, "voor de lol en omdat het technisch kan" en mensen die een statement willen maken. [13] [14] [15] De "capability" factor splitsen we op in de elementen: technische kennis & vaardigheden, doorzettingsvermogen, relevantie en de wil om financieel in de aanval te willen investeren.

[11] Lidar is "LIght Detection And Ranging" ook bekend als "Laser Imaging Detection And Ranging"
[12] Sherwood, J., 2004
[13] Gutierrez, M., 2014
[14] Oosterbaan, W., Lei van der G., 2014, p8
[15] Verizon, 2016, p 36

Als we deze capability elementen toepassen op de diverse categorieën mogelijke aanvallers dan ontstaat het volgende beeld.

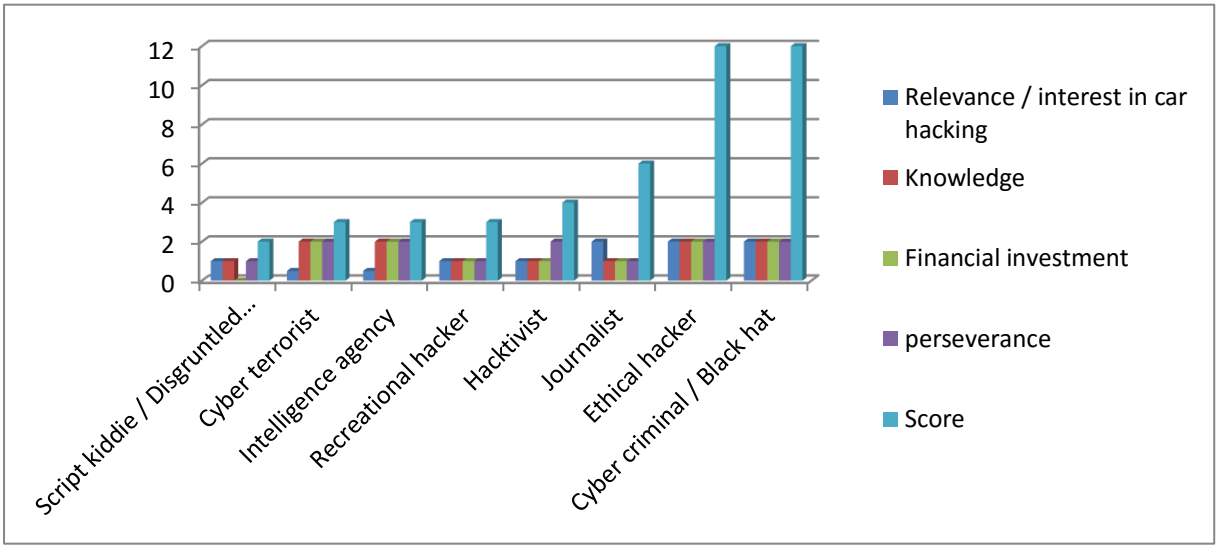

Fig 5. Actor analyse voor het hacken van auto's op basis van het SABSA model. [16]

Wat direct opvalt is dat de ethische hacker en de black hat hacker de grootste risico groep vormen. De black hat crimineel wil er financieel op vooruit gaan en de ethische hacker wil aantonen dat de huidige architectuur en configuratie van de connected auto niet cyber secure is. Door het publiceren van een "responsible disclosure" procedure [17] kan het risico van de ethische hacker effectief worden gemitigeerd. Het accepteren van externe hulp bij het identificeren en oplossen van bestaande kwetsbaarheden vergt bij sommige bedrijven een cultuuromslag.

In het derde deel van het onderzoek zijn de verzamelde resultaten van de eerste twee delen gecombineerd. Wij definiëren concrete stappen die de actoren in de automotive sector zelf kunnen nemen om auto's cyber secure te maken. De totale automotive keten moet hierin haar verantwoordelijkheid nemen. We behandelen achtereenvolgens: de autofabrikant, overheid, verzekeraars, brancheorganisaties, netwerk providers en eindgebruikers. In dit artikel noemen we de adviezen op hoofdlijnen, in het onderzoek staat een meer gedetailleerde roadmap per actor beschreven.

[16] Formule: relevantie * (technische kennis & vaardigheden + bereidheid tot financiële investeringen + doorzettingsvermogen) = score. Elementen zijn gewogen op basis van beschikbare literatuur.
[17] Een "responsible disclosure procedure" is een met waarborgen omklede procedure waarbij men op een verantwoordelijke manier de gevonden kwetsbaarheden in software openbaar maakt. NCTV, Nationaal Coördinator Terrorismebestrijding en Veiligheid "Leidraad Responsible Disclosure" https://www.nctv.nl/actueel/nieuws/2015/Responsibledisclosurekansvoordigitalesamenleving.aspx

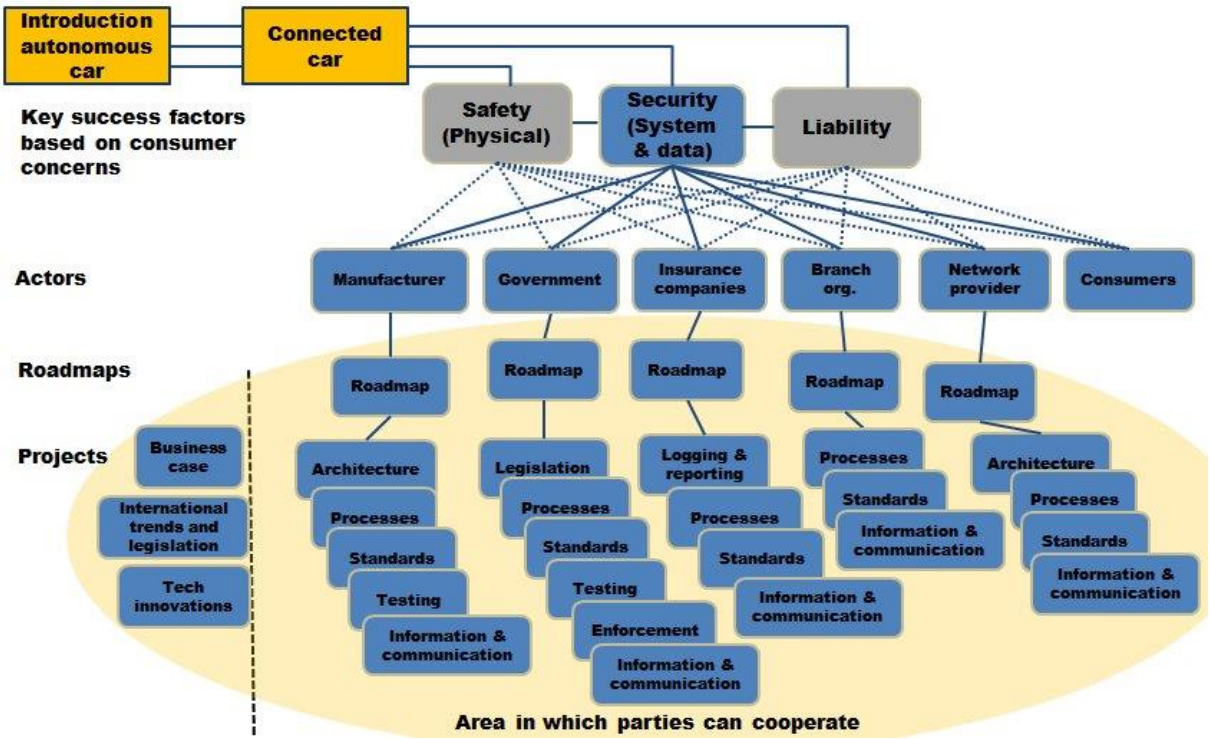

Fig 6. Multi actor diagram met de actoren die bij kunnen dragen een verbetering van de cyber security van auto's.

De autofabrikanten moeten de moderne auto gaan zien als een computer op wielen. Deze herdefiniëring heeft directe impact op de interne ICT architectuur van de auto. Een volgende stap is het uitvoeren en publiceren van cyber security testen. Tevens kan men een responsible disclosure policy opstellen en publiceren. Men moet ethische hackers de credits geven die ze verdienen in, bijvoorbeeld, een Europese "hall of fame". Voor sommige bedrijven vergt dit een cultuuromslag. Software ontwikkelaars begrijpen dat ingebakken "easter eggs" [18]niet grappig zijn, maar een teken van slecht testen en gebrek aan procedures en kwaliteit. "Security by design" zou de gouden standaard moeten zijn bij het programmeren van software.

Er is ook een duidelijke taak weggelegd voor de overheid. Dit geldt voor elke overheid die het gebruik van connected auto's en autonoom rijdende auto's wil reguleren. In dit onderzoek hebben we ons gericht op de Nederlandse overheid. Niet alleen moet er adequate wetgeving worden opgesteld over aansprakelijkheid en weggebruik, maar ook dient de overheid de kaders te geven waarin de automotive industrie zich mag bewegen. Zonder deze kaders is er een verlammende onzekerheid die de automotive industrie niet zelf kan oplossen en invullen. Fabrikanten willen wel investeren in de cyber security van auto's, maar dan wel met de zekerheid dat het geen weggegooid geld is. Zo moet de overheid de vraag beantwoorden van wie de data is die de connected auto verzameld. Nu is het zo dat

[18] Easter eggs zijn bewust door de software ontwikkelaar ingebouwde niet functionele features in software. Een voorbeeld hiervan is de "rainbow road" in de display van de Tesla Model S.

de verzamelde data naar diverse partijen gaat en de eindgebruiker zich daar niet bewust van is. Ook in het kader van de GDPR [19] is dat een interessant vraagstuk.

Een tweede vraagstuk is hoe lang de autofabrikant de software van de auto moet updaten en bijwerken. Het antwoord op deze vraag direct invloed op de business case van autofabrikanten. We zagen al dat de auto een rijdende computer is die mogelijk kwetsbaarheden bevat. De gemiddelde leeftijd van een personenauto in Nederland is 10 jaar.[20] Een “state of the art” computer is technisch afgeschreven in 3 jaar en over 10 jaar is zo’n computer zeker verouderd. Computers van 10 jaar oud zullen tegen die tijd ook zeker diverse security kwetsbaarheden bevatten. Hoe gaat de autofabrikant dit vraagstuk oplossen? Er zijn diverse oplossingen mogelijk. Zo kan men denken aan het afsluiten van betaalde security-abonnementen met de consument, onveilige functies in de auto (softwarematig) uitzetten, of alles gratis blijven updaten en bijwerken tot het laatste model van de weg af is. De kosten van de diverse oplossingen verschillen. Ook is er een informatieve taak weggelegd voor de overheid. Een jaarlijkse informatiecampagne om de consument voor te lichten is aan te bevelen.

Verzekeraars zijn gebaat bij een vermindering van het aantal schade-uitkeringen. Om het risico van cyberaanvallen op auto’s goed te kunnen bepalen is er historische data nodig. Het advies is om dit soort data op een consistente en goed doorzoekbare wijze te archiveren zodat er trendanalyses op gedaan kunnen worden. Politie, justitie en de wetgever kunnen deze informatie gebruiken om beleid te maken en waar nodig aan te scherpen.

Stichtingen, verenigingen, speciale belangen groepen en andere organisaties die actief zijn in de automotive industrie scharen we in dit onderzoek onder het begrip “Brancheorganisaties”. Deze kunnen een grote rol spelen in het informeren over-en promoten van cyber security van connected auto’s. Een jaarlijkse hacking marathon van connected cars is bijvoorbeeld iets wat men kan organiseren. Sommige landen, zoals Canada, zijn al actief op dit punt. Een ander advies is om een Europees auto ISAC [21]op te richten. Hierin kan dan specifieke informatie worden uitgewisseld en gedeeld. Alleen als partijen samen gaan werken op het vlak van security kan men hackers voor blijven.

De betrokkenheid van de netwerk providers is een ander belangrijk element in het verder cyber secure maken van de connected car. Zo moet security een belangrijk onderdeel uitmaken van de nieuwe 5G standaard die nodig is om de communicatie

[19] GDPR, General Data Protection Regulation. Dat is Europese privacy regelgeving met directe werking in alle lidstaten.

[20] https://www.cbs.nl/nl-nl/nieuws/2016/20/personenauto-s-steeds-ouder

[21] Auto ISAC, Automotive Information Sharing and Analysis Center https://www.automotiveisac.com/

van en naar voertuigen te verzorgen.

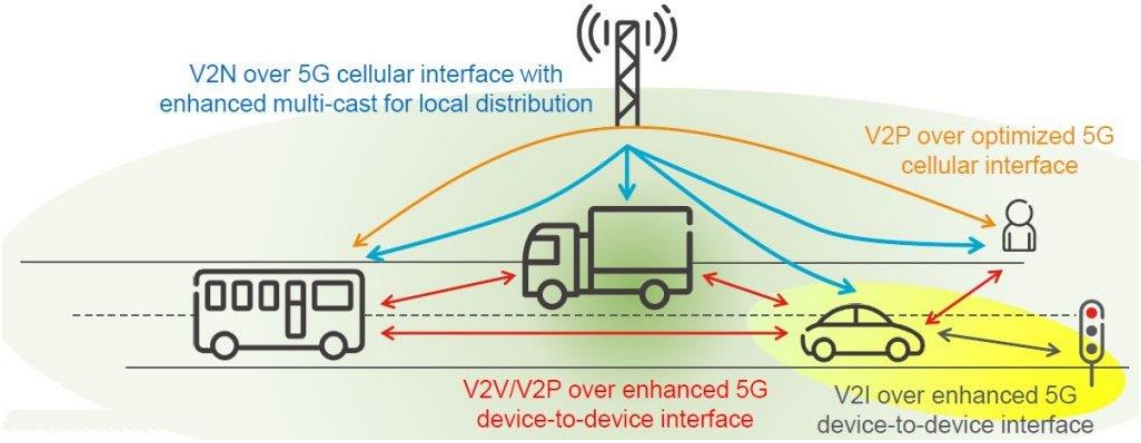

Fig 7. 5G communicatie gebaseerd op V2X (Dimitrovski, T., Sambeek, van M.; 2016, p 26)

Ten slotte hebben ook de eindgebruikers een rol. Zij moeten vragen gaan stellen aan hun volksvertegenwoordigers, de auto dealer en de autofabrikant over de cyber security van de auto.

Bibliography

1. CBS. (2015). CBS StatLine - Huishoudens in bezit van auto of motor; huishoudkenmerken. Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=81845ned&D1=1,3&D2=a&D3=0-2,13-31&D4=l&VW=T
2. CBS. (2016). CBS StatLine - Motorvoertuigenpark; inwoners, type, regio, 1 januari. Retrieved from http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=7374hvv&D1=2-11&D2=0&D3=a&HDR=T&STB=G2,G1&VW=T
3. Checkoway, S., Mccoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., … Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. *System*, 6–6. Retrieved from http://www.usenix.org/events/security/tech/full_papers/Checkoway.pdf
4. Dimitrovski, T. et al. (2016). *TNO report Wi-Fi monitoring - Next Generation Hotspot Q3 2016*.
5. Gutierrez, M. (2014). The Insights into Car Hacking. Retrieved from http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/Car Hacking - eel 6931 final.pdf
6. Jiang, T., Petrovic, S., & Husain, S. (2015). Self-Driving Cars - Disruptive or Incremental ? *Applied Innovation Review*, (1), 3–22. Retrieved from http://cet.berkeley.edu/wp-content/uploads/Self-Driving-Cars.pdf
7. Oosterbaan, W. ; Lei. van der G. (2014). *Cybersecurity autonoom rijdende voertuigen*.
8. Sherwood, J. (2004). Enterprise Security Architecture - SABSA. *Information Systems Security*, *6*(4), 1–27. http://doi.org/10.1080/10658989809342548
9. Sherwood, N. A. (2015). *Enterprise security architecture: a business-driven approach*. Retrieved from http://proquest.safaribooksonline.com/?fpi=9781578203185

10. Smith, C. (2016). *Car Hackers Handbook. A Guide for the Penetration Tester*. *Nostarch*. Retrieved from https://www.nostarch.com/carhacking
11. TU Automotive. (2016). Cyber Security in the Connected Vehicle Report 2016, 1–46. Retrieved from www.tu-auto.com/cybersecurity-report
12. Valasek, C., & Miller, C. (2013). Adventures in Automotive Networks and Control Units. *Technical White Paper*, 1–99. Retrieved from http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
13. Verizon. (2016). 2016 Data Breach Investigations Report. *Verizon Business Journal*, (1), 1–65. http://doi.org/10.1017/CBO9781107415324.004
14. Volvo. (2016b). Volvo Cars to launch UK's largest and most ambitious autonomous driving trial - Volvo Car Group Global Media Newsroom. Retrieved May 12, 2016, from https://www.media.volvocars.com/global/en-gb/media/pressreleases/189969/volvo-cars-to-launch-uks-largest-and-most-ambitious-autonomous-driving-trial