Hacking the Highway: a Legal Framework on Cybersecurity of Automated Vehicles

Dr. Nynke Vellinga Faculty of Law, University of Groningen

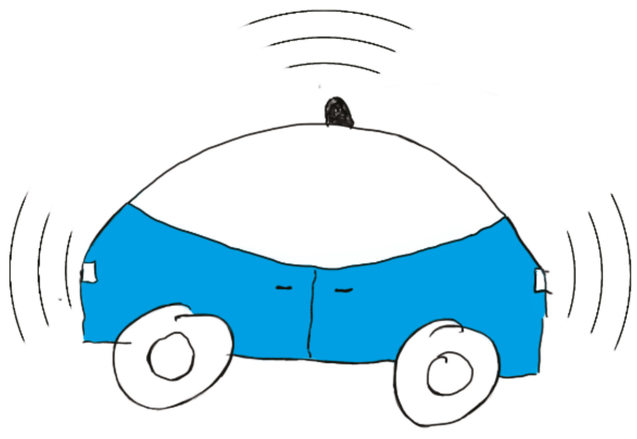
Automated Driving

Automated vehicles (AVs) are being developed in order to make road traffic **safer**. AVs can be completely self-driving, or they support the human driver in the performance of his driving task. In order to do so, AVs will need to **communicate** with their surroundings (infrastructure) and with other vehicles. Therefore, they need to be **connected**.

Cybersecurity

Connectivity, however, comes with an important **risk**; the risk of the exploitation of a **vulnerability**. If an AV gets hacked, the consequences could be detrimental. The hacker might be able to gain access to the **safety-critical** controls of the AV. The hacked AV could even be used in a **terrorist attack**.

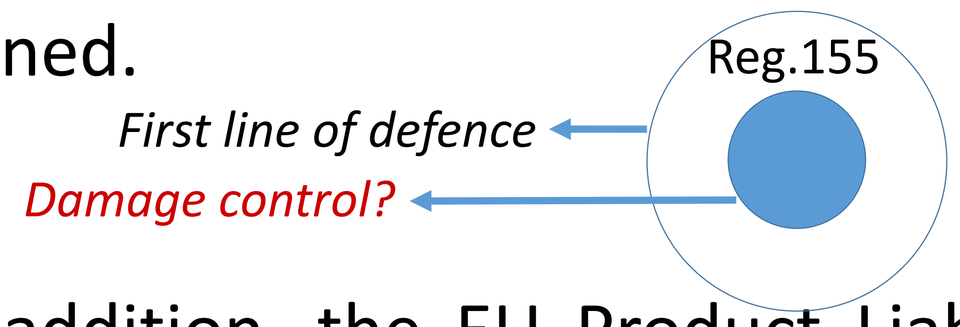
Thereby, cybersecurity enters the realm of road safety.



This requires a new **legal framework** on cybersecurity in automated vehicles.

Cybersecurity in AVs

Legislative steps have been taken to ensure cybersecurity in AVs. From 2022 onwards, all new vehicles in the EU have to be in conformity with UN Regulation 155 on cybersecurity in vehicles (EU Regulation 2019/2144). This, however, only forms a **first line of defence** as it is focused on how to prevent a hacker from gaining unauthorised access to the AV. Currently, there is no legislation on how to **control damage** once unauthorised access has been gained.



In addition, the EU Product Liability Directive leaves the question of whether and under what conditions a producer can be held **liable** for a cybersecurity breach unanswered.

Contact details

Questions or remarks?
Email address: **n.e.vellinga@rug.nl**

This research was funded by the CyberSecurity Noord-Nederland project. Twitter: @CybersecurityNN

university of groningen

PROGRAMMA CYBERSECURITY NOORD-NEDERLAND