CYBERSECURITY IN OVERDRIVE:

PREPARING FOR THE FUTURE OF AUTONOMOUS VEHICLES

December 11, 2017 - Russell House Office Building 385

The National Security Institute and the R Street Institute co-hosted a panel discussion on cybersecurity in the age of autonomous vehicles (AV). The panel examined the potential benefits and threats posed by AVs, as well as the regulatory approaches favorable to promoting public safety, consumer trust, and technological innovation.

DISCUSSION WRAP UP

The discussion focused on (1) the risks posed by AV cybersecurity failures, (2) the automotive industry's response to-date, and (3) recommended regulatory responses to these developing technologies.

Risks Posed by AV Cybersecurity Failures. The panelists began by providing various threat scenarios and their opinion on the likelihood of these incidents occurring. Mr. Watney explained that the increased complexity and connectivity of AVs raises the number of potential vectors an attacker could exploit and he warned of the physical harm that could come to drivers, bystanders, and infrastructure. He then introduced the risk of mass vulnerabilities – due to, for example, the penetration of a car's wireless communications – across entire fleets of vehicles, which could pose a nationwide risk. Mr. Watney conceded that the current risk of mass failures is remote.

Mr. Bort focused on the financial risks associated with AV cybersecurity failures. He posited that previous AV cybersecurity failures have been largely financially motivated low-level theft crimes. Overall, Mr. Bort asserted that the capabilities of today's real-world attackers are relatively simple; for example, mimicking key fobs to steal cars. He did acknowledge, however, that more sophisticated tools do exist and that as the use of AVs becomes more wide-spread, greater geopolitical risks may arise.

SPEAKERS

BRYSON BORT
Founder & CEO, SCYTHE

HON. DAVID STRICKLAND
Counsel & Spokesperson, Self-Driving Coalition for Safer Streets

CALEB WATNEY
Technology Policy Associate, The R Street Institute

BEAU WOODS
Cyber Safety Innovation Fellow, Brent Scowcroft Center on International Security, Atlantic Council

Moderator:
BRENDAN BORDELAN
Technology Correspondent, National Journal

The panelists also discussed the data privacy concerns arising from the growing use of AVs. Mr. Bort explained that AVs constitute a new component in an individual's digital footprint and overall personal identity. Mr. Watney argued that the data privacy concerns raised by AVs are not vastly different from existing concerns; smartphones already carry the large amounts of an individual's personal information that would also be stored in AVs.

Automotive Industry Response To-Date. The panelists agreed that car manufacturers are taking the cyber risks associated with AVs very seriously. Mr. Bort shared that, in his experience, the automotive industry regularly engages with the security community, welcoming independent security research and crowd sourced vulnerability disclosure programs. Mr. Strickland and Mr. Woods added that manufacturers view both government enforcement practices, as well as risk of civil suits, as incentives to establishing and maintaining cybersecurity.

All the panelists also spoke to car manufacturers' awareness that consumer trust is essential to the public's acceptance of AV technology and the manufacturers' success. Likewise, they stressed that consumer acceptance of AV technology is key to its wide-spread future deployment.

Recommended Regulatory Responses to AVs. Mr. Watney provided recommendations for a flexible regulatory policy framework that promotes cybersecurity best practices; these recommendations are included in a paper he co-authored with Cyril Draffin, "Addressing New Challenges in Automotive Cybersecurity." These recommendations center on extending the National Highway Traffic Safety Administration's (NHTSA) Federal Motor Vehicle Safety Standards (FMVSS) post-market recall authority to AVs.

Essentially, under the FMVSS structure, if a vehicle or equipment is found to be not in compliance with a specific standard or otherwise constitutes an unreasonable risk to consumer safety, NHTSA uses its recall authority to force a manufacturer to fix the defect or to remove the car from the road.

Mr. Watney's proposed AV framework has four steps:

(1) A manufacturer submits a comprehensive written cybersecurity plan to NHTSA;
(2) NHTSA makes non-sensitive/non-confidential answers available to the public;
(3) NHTSA would, or would contract white-hat hacker groups to, selectively test manufacturer's cybersecurity systems; and
(4) If testing reveals a vulnerability that is inconsistent with a manufacturer's cybersecurity plan, NHTSA could use its recall authority to remedy the issue.

Mr. Woods applauded the recommendations and stated that they would allow for parallel technological experimentation and for the flourishing of different business models. Mr. Strickland called the recommendations "thoughtful" but pointed out that a NHTSA finding that a manufacturer is in compliance with a NHTSA-approved cybersecurity plan would not shield the manufacturer from liability if a failure were to occur.

Lastly, the panelists raised the issue of how civil agencies will work together on AV cybersecurity in the future. Due to the national security concerns implicated in AVs, as well as NHTSA's limited technical cyber expertise, the panelists agreed that the Department of Defense, including Cyber Command, Department of Homeland Security, Department of Justice, and local and state law enforcement officers will need to work alongside NHTSA.