Negative: Cybersecurity for Autonomous Cars

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan has the federal government mandate cybersecurity testing standards for autonomous cars.

Negative: Cybersecurity for Autonomous Cars 3

TOPICALITY 3

1. Extra-topical mandates. Plan goes beyond the resolution with mandates on things that aren’t AI 3

Link: AFF advocate Suchodolski (NC Journal of Law & Technology 2018) says her cybersecurity plan involves AASD (autonomous and automatic systems and devices) 3

Link: Suchodolski says AASD includes things that aren’t AI, like tire pressure sensors and everything from that up to fully autonomous cars 3

Link: Suchodolski never mentions AI 3

Violation: They’re affirming the wrong resolution. Plan reforms “cars” not “AI” 3

Impact: Abuse to the Negative team justifies a Negative ballot 3

2. Not substantial reform 4

Link: AFF Plan implements the AV START Act 4

Link: The AV START Act would not be a radical departure from the Status Quo approach to autonomous vehicle cybersecurity 5

Violation: Trivial changes are not substantial reforms 5

Impact: Abuse justifies a Negative ballot 5

INHERENCY 6

1. Existing NHTSA authority 6

National Highway Traffic Safety Administration (NHTSA) has authority to solve Automated Driving System (ADS) risks in Status Quo 6

2. The “Uptane” system 6

Uptane already exists in Status Quo and provides security against attacks 6

Definition of Uptane 6

3. Existing Over The Air (OTA) update systems solve 7

Existing OTA already has methods to patch security flaws well enough to outweigh security concerns 7

4. Customer demand & industry response 7

Manufacturers respond quickly to cyber security concerns because people won’t buy their cars if they can’t trust them 7

Federal regulatory standards won’t move fast enough, but that’s OK: They add nothing to existing industry goals for safety, because untrusted technology won’t sell 7

HARMS / SIGNIFICANCE 8

1. Hacking risk is low 8

Risk of hacking on cars is low and impacts easily avoided 8

SOLVENCY 8

1. No enforcement 8

Plan doesn’t actually require removing non-compliant cars from the road 8

2. More study needed 8

Very little is known about the impact of cyber attacks on transportation and current studies aren’t enough (July 2021) 8

Cyber attack reduction planning is “useless” without more study first 9

A/T “But our Plan has more study!” – More study isn’t reform, so it’s extra-topical. Only a NEG ballot gets more study 9

DISADVANTAGES 9

1. Delays autonomous car acceptance 9

Link: Plan requires increased publicity of failures 9

Link: Publicity of failures reduces public acceptance, distracts from the benefits, and slows rollout 9

Impact: Lives and Money. Every year of delay costs thousands of lives and billions of dollars 10

Works Cited 11

Negative: Cybersecurity for Autonomous Cars

TOPICALITY

1. Extra-topical mandates. Plan goes beyond the resolution with mandates on things that aren’t AI

Link: AFF advocate Suchodolski (NC Journal of Law & Technology 2018) says her cybersecurity plan involves AASD (autonomous and automatic systems and devices)

Affirmative source Jeanne Suchodolski 2018 (J.D.; LLM) N.C. JOURNAL OF LAW & TECHNOLOGY Cybersecurity of Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms 1 Oct 2018 <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1364&context=ncjolt> (accessed 16 Dec 2021)

The future promises fully autonomous devices such as unmanned aerial systems (“UAS”) and self-driving cars (“UAV”). These autonomous and automatic systems and devices (“AASD”) provide safety, efficiency, and productivity benefits. Yet AASD operate under continual threat of cyber-attack.

Link: Suchodolski says AASD includes things that aren’t AI, like tire pressure sensors and everything from that up to fully autonomous cars

Affirmative source Jeanne Suchodolski 2018 (J.D.; LLM) N.C. JOURNAL OF LAW & TECHNOLOGY Cybersecurity of Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms 1 Oct 2018 <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1364&context=ncjolt> (accessed 16 Dec 2021)

AASD may comprise an entire vehicle, or a self-contained component or subsystem thereof. The degree of automation within AASD spans a wide range. At their least complex, AASD involve the simple automatic monitoring of a component or subsystem: for example, the tire pressure sensor and its companion alert system on a car. At their most complex, AASD include completely autonomous operations like self-driving cars. Between these two extremes lies automatic and autonomous systems such as flight management computers, ships’ autopilots, and the vehicle chassis control used to manage road handling. The principal distinctions between an automatic system and an autonomous system are the degree of complexity and the impact on the overall operation and conduct of the apparatus of which it forms a part. For purposes of this paper, an automatic system, subsystem, component, or device is one capable of operating without external control or intervention (e.g. a tire pressure warning light), while an autonomous system is self-governing with logic that enables decision making independent of human intervention (e.g. an unmanned aircraft that delivers packages to your doorstep). The consequences of a cyberattack depends in part upon the degree of automation as well as the function of the device or system automated.

Link: Suchodolski never mentions AI

You won’t find Artificial Intelligence anywhere in their Suchodolski NC Journal of Law & Technology 2018 evidence. That’s because in her entire 78-page article the words “artificial intelligence” never appear even once.

Violation: They’re affirming the wrong resolution. Plan reforms “cars” not “AI”

The Affirmative is advocating cybersecurity for “cars,” not for AI, because that’s what their expert says. But this is the wrong resolution for that plan. If the resolution said the federal government should improve transportation safety, this plan would be topical. But the resolution limits us to only debating AI, and their plan goes way beyond that. They’re doing “the resolution plus a lot more” to achieve the benefits of their plan.

Impact: Abuse to the Negative team justifies a Negative ballot

We came prepared to debate AI, not “AI plus everything else.” Letting an Affirmative win by affirming other things in addition to the resolution is abusive to Negative teams and by itself warrants a Negative ballot.

2. Not substantial reform

Link: AFF Plan implements the AV START Act

**The following quote references two footnotes, number 246 and 247 in the original article. After reading the quote, I’ll then read those footnotes because they link the AFF plan to the AV START Act.**

Affirmative source Jeanne Suchodolski 2018 (J.D.; LLM) N.C. JOURNAL OF LAW & TECHNOLOGY Cybersecurity of Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms 1 Oct 2018 <https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1364&context=ncjolt> (accessed 16 Dec 2021)

For perhaps this reason, or in response to the specific drawbacks noted above, current legislation pending in Congress would make the now voluntary self-assessment of compliance with these standards compulsory while prohibiting the States from levying additional design standards.246 In addition, each proposed bill requires mandatory cybersecurity plans from automobile manufacturers documenting their process for identifying and mitigating vulnerabilities to cyber-attack.247

 **FOOTNOTE 246:**

246 See AV Start Act, S. 1885, 115th Cong. (2017); H.R. 3388, 115th Cong. (2017) (requiring that manufacturers of highly automated vehicles develop written cybersecurity and privacy plans for such vehicles prior to offering them for sale, and also mandating that the Department of Transportation require safety assessment certifications for the development of a highly automated vehicle or an automated driving system). The proposed legislation also amends 49 U.S.C. § 30103 (b) to preempt any State laws or regulations regarding the design or construction of automated vehicles.

**FOOTNOTE 247:**

247 Id. The proposed legislation is an attempt to amend Chapter 301, subtitle VI of 49 U.S.C. by inserting a new section, § 30130 Cybersecurity of automated driving systems. See H.R.3388, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/3388/summary/00, for the language as specifically proposed.

Link: The AV START Act would not be a radical departure from the Status Quo approach to autonomous vehicle cybersecurity

Caleb Watney and Cyril Draffin 2017. (Caleb Watney is a technology policy associate at the R Street Institute, where he leads R Street’s work on emerging technologies, including autonomous vehicles, artificial intelligence, drones, robotics and medical tech.. Cyril Draffin project adviser to the MIT Energy Initiative. He evaluates the cybersecurity of electric utilities. He is U.S. representative to the International Energy Agency International Smart Grid Action Network Academy, was cybersecurity lead for MIT Energy Initiative “Utility of the Future” study, member of the Maryland Cybersecurity Council) R STREET POLICY STUDY: 2017 ADDRESSING NEW CHALLENGES IN AUTOMOTIVE CYBERSECURITY <https://www.bafuture.org/sites/default/files/key-topics/attachments/Addressing%20Automotive%20Cybersecurity%20Nov%202017.pdf> (accessed 16 Dec 2021)

To date, the most significant push for a federal legislative framework specifically for connected and autonomous cars has come this year with the House’s SELF DRIVE Act and the Senate’s AV START Act. Each proposal is broadly aimed at clearing regulatory hurdles for the deployment of autonomous vehicles and both include specific sections with respect to cybersecurity. In exchange for broad pre-emption from state and local regulations on the security, design and performance of autonomous vehicles, both of these bills take the voluntary safety self-assessment letter that NHTSA developed as part of its FAVP and make it mandatory. In addition, they each require written cybersecurity plans from auto manufacturers that “cover a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands.” Additionally, the AV START Act’s cybersecurity section requires manufacturers to answer a few additional questions about their cybersecurity practices and authorizes the DOT to create incentives for voluntary disclosure of vulnerabilities. However, the bills are fairly consistent in their overall content. If one of these bills (or a unified version which emerges from a conference committee) becomes law, it would not be a radical departure from the NHTSA’s existing cybersecurity approach.

Violation: Trivial changes are not substantial reforms

We’re supposed to be debating substantial reforms, not minor repairs to the Status Quo.

Impact: Abuse justifies a Negative ballot

We need to teach Affirmatives not run tiny plans that they hope no one will have evidence on. The word “substantial” is in the resolution for a reason and it’s to stop Affirmatives from running trivial plans like this one. It’s abusive to Negatives because the research burden would be infinite if you let Affirmatives run any tiny change they want to.

INHERENCY

1. Existing NHTSA authority

National Highway Traffic Safety Administration (NHTSA) has authority to solve Automated Driving System (ADS) risks in Status Quo

National Highway Traffic Safety Administration 2017 (agency of the US Dept of Transportation) AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY, Sept 2017 (accessed 16 Dec 2021) https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0\_090617\_v9a\_tag.pdf

Several States have sought clarification of NHTSA’s enforcement authority with respect to ADSs. As DOT is asking States to maintain the delineation of Federal and State regulatory authority, NHTSA understands that States are looking for reassurance that the Federal Government has tools to keep their roadways safe. NHTSA has broad enforcement authority to address existing and new automotive technologies and equipment. The Agency is commanded by Congress to protect the safety of the driving public against unreasonable risks of harm that may arise because of the design, construction, or performance of a motor vehicle or motor vehicle equipment, and to mitigate risks of harm, including risks that may arise in connection with ADSs. Specifically, NHTSA’s enforcement authority concerning safety-related defects in motor vehicles and motor vehicle equipment extends and applies equally to current and emerging ADSs.

2. The “Uptane” system

Uptane already exists in Status Quo and provides security against attacks

Amit Agarwal 2020 (with PathPartner - a specialist in product engineering, providing concept-to-production services to customers across automotive, consumer electronics, broadcast, medical and internet-of-things domains ) Understanding Automotive OTA (Over-the-Air Update) 26 June 2020 <https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update/> (accessed 17 Nov 2021)

**OTA update using Uptane**
The Update Framework (TUF) is designed to create a security system to protect users of software repositories from the security attacks. It has been designed, keeping in mind that the backend server may not be secure, or the key used for the cryptography can be stolen. So, what it does is it creates a distributed system, where the dependency on a particular system is not there, and in case of the attacker’s thread, all the systems cannot be hacked so easily at the same time. The Update Framework (TUF) has divided the roles into four parts (Root of trust, Timestamps, Snapshot, Targets) Uptane builds on The Update Framework (TUF), which is distributed (Timeserver, directory and image repository, manifests, Primary/secondary ECU’s, full and partial verification.

Definition of Uptane

Amit Agarwal 2020 (with PathPartner - a specialist in product engineering, providing concept-to-production services to customers across automotive, consumer electronics, broadcast, medical and internet-of-things domains ) Understanding Automotive OTA (Over-the-Air Update) 26 June 2020 (brackets added) <https://www.pathpartnertech.com/understanding-automotive-ota-over-the-air-update/> (accessed 17 Nov 2021)

The most challenging part of the component is when the data/Images are exposed to the n/w [network] and they are easy for the attackers to manipulate. There are many techniques, open-source and third-party solution for secure update to the head unit Most commonly used is Uptane. Uptane is the first comprehensive security framework guiding the implementation of OTA update systems on a design level.

3. Existing Over The Air (OTA) update systems solve

Existing OTA already has methods to patch security flaws well enough to outweigh security concerns

Keith Barry 2018 (car writer for Consumer Reports) Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair? 20 Apr 2018 <https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/> (accessed 17 Nov 2021)

If a hack does happen at some point in the future, though, Koscher says that OTA updates should make it easier to fix—much the same way that your phone or computer can patch a security flaw with a software update. “The security concern will be outweighed by the ability to catch security issues,” Koscher says.

4. Customer demand & industry response

Manufacturers respond quickly to cyber security concerns because people won’t buy their cars if they can’t trust them

Kareem Othman 2021. (Research Assistant, Civil Engineering Dept, Univ. of Toronto) Public acceptance and perception of autonomous vehicles: a comprehensive review, AI ETHICS, Feb 2021 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7908960/> (accessed 16 Dec 2021)

For example, in 2016, a team of researchers hacked a Tesla car and took control of the car for almost 12 miles. The Chinese researchers were able to control every electronic feature of the vehicle remotely such as brakes and car locking. The attack requires the car to be connected to a malicious Wi-Fi system set by the team and the attack can be done only if the car browser is opened. Tesla stated that the probabilities to meet the attack requirements were very low, but this would not stop them from responding quickly. In fact, cybersecurity represents a major concern for the public. Surveys showed high levels of concerns regarding security as follows:
- 90.9% of respondents are concerned about vehicle security

* 54% of respondents are concerned about vehicle security
* 68% of respondents are concerned about vehicle security

As a result, vehicle security is an important feature to gain customers' trust.

Federal regulatory standards won’t move fast enough, but that’s OK: They add nothing to existing industry goals for safety, because untrusted technology won’t sell

Katie Pyzyk 2021 (journalist) 7 Sept 2021 “Are federal AV investigations a first step toward federal regulation? Not necessarily, experts say” <https://www.smartcitiesdive.com/news/federal-av-autonomous-vehicle-tesla-investigation-regulation/605963/> (accessed 17 Dec 2021) (bracket added)

If and when the regulatory environment does begin to change, it's unlikely to move fast enough to get ahead of the technology, [Mark] Fagan [lecturer in public policy at the Harvard Kennedy School] says. "They are not getting ahead of this. It is the reason that state and local governments have established regulations around testing, operations and the like, because there is no federal guideline," he said. "State and local governments are essentially filling that vacuum." Plus, most proposed federal AV regulations to date are in line with industry goals because they center on AV companies' top priority — safety —[vice president of policy and finance at the Eno Center for Transportation, Paul] Lewis said, not only to protect customers but also because untrusted technology won't sell.

HARMS / SIGNIFICANCE

1. Hacking risk is low

Risk of hacking on cars is low and impacts easily avoided

Doug Newcomb 2020 (journalist) 6 Nov 2020 “The Upsides and Downside of Over-the-Air Software Updates for Automobile Dealers” <https://www.wardsauto.com/dealers/upsides-and-downside-over-air-software-updates-automobile-dealers> (accessed 17 Nov 2021)

OTA updates also provide a gateway for hackers, although most security experts agree remotely accessing a car’s critical systems is very difficult and time-consuming. They also point out there’s currently far less incentive to hack a car compared to, say, accessing someone’s bank account. And security concerns could be outweighed by the ability to catch and fix security issues more quickly. If a hack occurs, OTA updates make it easier for a vehicle to protect itself in the same way phones and computers patch a security flaw with a software update.

SOLVENCY

1. No enforcement

Plan doesn’t actually require removing non-compliant cars from the road

Caleb Watney and Cyril Draffin 2017. (Caleb Watney is a technology policy associate at the R Street Institute, where he leads R Street’s work on emerging technologies, including autonomous vehicles, artificial intelligence, drones, robotics and medical tech.. Cyril Draffin project adviser to the MIT Energy Initiative. He evaluates the cybersecurity of electric utilities. He is U.S. representative to the International Energy Agency International Smart Grid Action Network Academy, was cybersecurity lead for MIT Energy Initiative “Utility of the Future” study, member of the Maryland Cybersecurity Council) R STREET POLICY STUDY: 2017 ADDRESSING NEW CHALLENGES IN AUTOMOTIVE CYBERSECURITY https://www.bafuture.org/sites/default/files/key-topics/attachments/Addressing%20Automotive%20Cybersecurity%20Nov%202017.pdf

Additionally, the AV START Act’s cybersecurity section requires manufacturers to answer a few additional questions about their cybersecurity practices and authorizes the DOT to create incentives for voluntary disclosure of vulnerabilities. However, the bills are fairly consistent in their overall content. If one of these bills (or a unified version which emerges from a conference committee) becomes law, it would not be a radical departure from the NHTSA’s existing cybersecurity approach. It would certainly be the first time that auto manufacturers are required to submit a full cybersecurity plan before deploying connected vehicles, but the NHTSA would be barred from keeping cars off the road based solely on their answers to those cybersecurity questions. Practically speaking, this would be more of an information-sharing arrangement than a traditional regulatory one. There could certainly be scenarios where manufacturers change their practices or behavior because they know their answers are being read by regulators, but this process would look more like an experiment in soft law than hard law.

2. More study needed

Very little is known about the impact of cyber attacks on transportation and current studies aren’t enough (July 2021)

Ian McManus 2021 (Master of Science candidate at Virginia Polytechnic Institute and State University) The Impact of Cyberattacks on Safe and Efficient Operations of Connected and Autonomous Vehicles, 29 July 2021 <https://vtechworks.lib.vt.edu/bitstream/handle/10919/104891/McManus_IP_T_2021.pdf?sequence=1> (accessed 16 Dec 2021) (brackets added)

Very little is known about the impact of cyberattacks on traditional transportation engineering metrics like safety and operations. Generally, research that has been conducted on the topic was from an electrical or computer science lens which neglects the transportation network impact of the attacks. These studies have examined the impacts of attacks on the VANET [vehicular ad hoc network] itself and recommending countermeasures to specific attacks, but not translating it to transportation - or not sufficiently doing so.

Cyber attack reduction planning is “useless” without more study first

Ian McManus 2021 (Master of Science candidate at Virginia Polytechnic Institute and State University) The Impact of Cyberattacks on Safe and Efficient Operations of Connected and Autonomous Vehicles, 29 July 2021 <https://vtechworks.lib.vt.edu/bitstream/handle/10919/104891/McManus_IP_T_2021.pdf?sequence=1> (accessed 16 Dec 2021) (brackets added)

The overarching goal for this research is that the results can be used in a risk assessment while planning for a robust and resilient connected transportation network in the future. The results show what could happen if cybersecurity is ignored through ITS [Intelligent Transportation System] and CAV [Connected & Autonomous Vehicles] implementation. Understanding the impact an attack is first step in planning against it, and without a proper understanding, a resilience plan is essentially useless against the impact.

A/T “But our Plan has more study!” – More study isn’t reform, so it’s extra-topical. Only a NEG ballot gets more study

Doing study is great, but you only get it with a Negative ballot. AFF cannot do “more study” because the resolution requires substantial reform. Study doesn’t reform anything, so it has to be dropped from the AFF Plan if they’re claiming it. It’s extra-topical.

DISADVANTAGES

1. Delays autonomous car acceptance

Link: Plan requires increased publicity of failures

It’s in their mandates

Link: Publicity of failures reduces public acceptance, distracts from the benefits, and slows rollout

Center for the Study of the Presidency and Congress 2017 (non-profit, non-partisan research group) THE AUTONOMOUS VEHICLE REVOLUTION MARCH 2017 FOSTERING INNOVATION WITH SMART REGULATION <https://www.ftc.gov/system/files/documents/public_comments/2017/03/00002-140353.pdf> (accessed 17 Dec 2021)

Political perceptions and regulatory regimes surrounding autonomous vehicles will be significant factors in determining whether this technology reaches its full potential. Difficulties encountered in testing or heavily publicized faults in the technology could present perception problems. Throughout the development of this technology, it will be vital that technology developers, autonomous vehicle advocates, and political and regulatory leaders remain focused on the potential benefits of this technology. Difficulties inherent in the deployment of any new technology are inevitable. The potential of this transformational technology should not be overshadowed by near-term challenges.

Impact: Lives and Money. Every year of delay costs thousands of lives and billions of dollars

Caleb Watney and Cyril Draffin 2017. (Caleb Watney is a technology policy associate at the R Street Institute, where he leads R Street’s work on emerging technologies, including autonomous vehicles, artificial intelligence, drones, robotics and medical tech.. Cyril Draffin project adviser to the MIT Energy Initiative. He evaluates the cybersecurity of electric utilities. He is U.S. representative to the International Energy Agency International Smart Grid Action Network Academy, was cybersecurity lead for MIT Energy Initiative “Utility of the Future” study, member of the Maryland Cybersecurity Council) R STREET POLICY STUDY: 2017 ADDRESSING NEW CHALLENGES IN AUTOMOTIVE CYBERSECURITY https://www.bafuture.org/sites/default/files/key-topics/attachments/Addressing%20Automotive%20Cybersecurity%20Nov%202017.pdf

The potential benefits offered by both connected and autonomous vehicles are far-ranging and substantial. Most significantly, they provide an opportunity to save thousands of lives a year and to reduce the economic and social costs of auto accidents. Drunk, drowsy and distracted driving contributed to 40,000 auto fatalities last year. Worse still, this number is increasing, as is the urgency to address it. According to the National Highway Traffic Safety Administration (NHTSA), the first half of 2016 experienced a 10.6 percent rise in the number of automobile fatalities compared to the same period of the previous year. Among young people, vehicle-related fatalities are the nation’s single most profound public health crisis. Because an estimated 94 percent of accidents are the result of human error, autonomous and connected vehicles have the opportunity to save tens of thousands of lives and hundreds of billions of dollars each year.

Works Cited

1. ABC News 2018. (writer is Julia Macfarlane. She is a London-based reporter covering global affairs for ABC News. She began her career as a freelance photojournalist working in Indonesia, where she was born. She then moved to Beirut, Lebanon and worked for the BBC News bureau as a producer and TV journalist. A graduate of University of St. Andrews in Scotland, Macfarlane received her MA in English Literature.) 2 February 2018 “Why is the US still in Afghanistan?” https://abcnews.go.com/International/us-afghanistan/story?id=52763044