

RESEARCH SOURCE LIST

Dear Mr. Sloat:

Please see resources below for a “cyjacking” law review article. For readability purposes, I have put the source first, and then a brief summary of the contents and its relevance to the article below. I am happy to start drafting a background section for a law review article if you’d like or can continue further research and draft a memo.

I. Hijacking

A. Generally, History

- Janet Bednarek for The Conversation, *A Brief History of Airplane Hijackings, From the Cold War to D.B. Cooper*, SMITHSONIAN MAGAZINE (July 18, 2022), <https://www.smithsonianmag.com/history/a-brief-history-of-airplane-hijackings-db-cooper-netflix-180980408/>
Details the history of hijacking, including the Peru hijack and D.B. Cooper hijack. The article also describes case law on expanded security measures to address aircraft hijacking.
- *Today in History: The First Hijack*, THE RETROSPECTORS, <https://theretrospectors.com/the-first-hijack/>
Podcast and provisional text providing a quick summary of the first recorded hijacking, which is also mentioned in the Smithsonian article.
- Kirsten Ford, “Get to the Chopper!” *The Incredible Tale of the Mountjoy Prison Helicopter Escape*, TALES FROM THE UNDERWORLD (Feb. 09, 2025), <https://www.talesfromtheunderworld.com/p/get-to-the-chopper-the-incredible>
This article describes a prison break in Ireland that used a hijacked helicopter to assist in the escape.
- Sarah Slater, *Man Behind Helicopter Hijacking that Airlifted IRA Prisoners Out of Mountjoy Shares Story*, BREAKING NEWS.IE (Aug. 9, 2021), <https://www.breakingnews.ie/ireland/man-behind-helicopter-hijacking-that-airlifted-ira-prisoners-out-of-mountjoy-shares-story-1181666.html>
This article provides another perspective on the Mountjoy helicopter hijacking prison break.

B. Prosecuting Hijackers

- William G. Phelps, *Validity, Construction, and Application of Provisions of Federal Aviation Act (49 U.S.C.A. Appx. §§ 1472(i)(l),(n)) Punishing Air Piracy and Certain Acts Aboard Aircraft in Flight, or Boarding Aircraft*, 109 A.L.R. Fed. 488 (1992).
ALR report on punishing air piracy, but has limiting “aboard aircraft” language.

II. Hacking in General

- Jacob Fox, *A Brief History of Hacking*, COBALT (Dec. 5, 2022), <https://www.cobalt.io/blog/history-of-hacking>
Details the history of hacking, and its origins in telecommunications.
- *Significant Cyber Incidents*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
A very long and comprehensive list of notable cyber incidents in history.

III. Hacking Self-Driving Cars

- David Drucker, *Protecting Your Self-Driving Car – And Your Privacy – From Cyberhackers in the Age of AI*, FLORIDA INTERNATIONAL UNIVERSITY NEWS (Aug. 7, 2023), <https://news.fiu.edu/2023/how-ai-will-protect-your-car-and-your-privacy>
This article describes the risks of hacking cars with computerized features, and how safety and data privacy are both top concerns. This is relevant to our research because though safety is the top priority for the AAM industry, if a malicious actor hacked an AAM aircraft, there might be additional risks to things like data privacy and security.
- *Six Ways to Protect Against Autonomous Vehicle Cyber Attacks*, IEEE INNOVATION AT WORK, <https://innovationatwork.ieee.org/six-ways-to-protect-against-autonomous-vehicle-cyber-attacks/>
This article provides tips against autonomous vehicle hacking, some of which could be applied to the AAM industry.
- Se In Jung and Shin Dong Hu, *A Study on Hacking Attacks and Vulnerabilities in Self-Driving Car With Artificial Intelligence*, <https://ieomsociety.org/proceedings/2022orlando/249.pdf>
This paper describes autonomous vehicle technology, and the specifics on how hackers could potentially take control of an autonomous vehicle. The article also provides suggestions on how to protect against hackers.

- Emmet White, *Autonomous Vehicles are Vulnerable to Lidar Hacking, Researchers Say*, AUTOWEEK (Mar. 1, 2024), <https://www.autoweek.com/news/a60043383/autonomous-vehicles-hacking-spoofing/>
This article describes lidar risks for autonomous vehicles. Malicious actors can interfere with lidar return lasers, creating potential for “abrupt, unnecessary, and dangerous driving behavior from autonomous vehicles.”
- WIRED, *Hackers Remotely Kill a Jeep on the Highway*, WIRED (July 21 2015), <https://www.youtube.com/watch?v=MK0SrxBC1xs>
Visual example of how hackers can impact even the most basic forms of technology in cars found in cars a decade ago. Hackers showed how they could remotely hack a 2014 Jeep Cherokee and its steering, transmission, and other systems via cellular connection.
- Alex Vakulov, *Cybersecurity Threats To Modern Cars: How Hackers Are Taking Control*, FORBES (Jan. 25, 2025), <https://www.forbes.com/sites/alexxvakulov/2025/01/25/cybersecurity-threats-to-modern-cars-how-hackers-are-taking-control/>
This article describes a flaw in Subaru’s Starlink system that could allow hackers to control cars just by obtaining the vehicle’s license plate and basic driver information.
- *Hacking Subaru: Tracking and Controlling Cars via the STARLINK Admin Panel*, SAMCURRY.NET (Jan. 23, 2025), <https://samcurry.net/hacking-subaru>
This is the project mentioned in the Forbes article above. Goes into greater detail on the method and the potential dangers, including the fact that “an attacker who only knew the victim’s last name and ZIP code, email address, phone number, or license plate could . . . [among other things, retrieve] any vehicle’s complete location history from the past year.”