NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FULLY AUTONOMOUS VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVICES—MITIGATING STRATEGIES

by

Kevin S. Knopf

March 2019

Co-Advisors:	Robert L. Simeral Thomas Mackin, CalPoly, San Luis Obispo

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE FULLY AUTONOMOUS VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVICES—MITIGATING STRATEGIES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Kevin S. Knopf	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The technology integrated into fully autonomous vehicles will soon be a significant homeland security threat. Companies ranging from major corporations to small startups are investing billions of dollars developing this technology. It is currently predicted that fully autonomous vehicles will be available to the general public within a matter of years. As fully autonomous vehicles become broadly available both to the general public and private entities, significant impacts will likely result to our safety, both as individuals and as a community. This thesis overviews the projected threat posed by the nefarious use of fully autonomous vehicles as fully autonomous vehicle-borne improvised explosive devices. It is shown how easily autonomous vehicles can be used for explosive delivery and discusses technological solutions that should be implemented, proactively, to reduce this threat. A pressing need exists for secure communications, user authentication, law enforcement override, and payload interrogation that must be implemented at the outset of the system design process. Absent a security-based systems design approach, this nation will be reacting to, rather than preventing, the use of autonomous vehicles as explosive delivery systems. The overarching purpose of this thesis is also to capture what can be accomplished with public-private partnerships working collaboratively to address strategic issues involving public safety in the United States.

14. SUBJECT TERMS autonomous vehicles, connected vehicle technology, Internet of things, self-driving vehicle, driverless vehicle, automated vehicle, self-driving car, driverless car, automated car, law enforcement, law enforcement policy, public safety, vehicle-borne explosive device, VBIED, car bomb, fully autonomous vehicle-borne improvised explosive device, FAVBIED, public-private partnership, homeland security, homeland security enterprise	**15. NUMBER OF PAGES** 123
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

FULLY AUTONOMOUS VEHICLE-BORNE IMPROVISED EXPLOSIVE DEVICES—MITIGATING STRATEGIES

Kevin S. Knopf
Lieutenant, California Highway Patrol
BS, California Polytechnic State University, 1993
MPA, National University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2019**

Approved by: Robert L. Simeral
Co-Advisor

Thomas Mackin
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The technology integrated into fully autonomous vehicles will soon be a significant homeland security threat. Companies ranging from major corporations to small startups are investing billions of dollars developing this technology. It is currently predicted that fully autonomous vehicles will be available to the general public within a matter of years. As fully autonomous vehicles become broadly available both to the general public and private entities, significant impacts will likely result to our safety, both as individuals and as a community. This thesis overviews the projected threat posed by the nefarious use of fully autonomous vehicles as fully autonomous vehicle-borne improvised explosive devices. It is shown how easily autonomous vehicles can be used for explosive delivery and discusses technological solutions that should be implemented, proactively, to reduce this threat. A pressing need exists for secure communications, user authentication, law enforcement override, and payload interrogation that must be implemented at the outset of the system design process. Absent a security-based systems design approach, this nation will be reacting to, rather than preventing, the use of autonomous vehicles as explosive delivery systems. The overarching purpose of this thesis is also to capture what can be accomplished with public-private partnerships working collaboratively to address strategic issues involving public safety in the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADS	automated driving system
ANFO	ammonium nitrate-fuel oil
CONUS	continental United States
DHS	Department of Homeland Security
DIEDS	Domestic Improvised Explosive Device Subcommittee
DoJ	Department of Justice
ECU	electronic control unit
EDR	event data recorder
FAA	Federal Aviation Administration
FACV	fully autonomous commercial vehicle
FACVBIED	fully autonomous commercial vehicle borne improvised explosive device
FAV	fully autonomous vehicle
FAVBIED	fully autonomous vehicle-borne improvised explosive device
FBI	Federal Bureau of Investigation
GPS	global positioning satellite
IED	improvised explosive device
IoT	Internet of things
IRA	Provisional Irish Republican Army
JCAT	Joint Counterterrorism Assessment Team
NHTSA	National Highway Transportation Safety Agency
NSA	National Security Agency
R&D	research and development
ROI	return on investment
RPV	remotely piloted vehicle
SAE	Society of Automotive Engineers International
SUAV	small unmanned aerial vehicle
SVBIED	suicide vehicle-borne explosive device
TSA	Transportation Security Administration
UAS	unmanned aircraft system

UAV	unmanned aerial vehicle
V2I	vehicle- to-infrastructure
V2V	vehicle-to-vehicle
V2X	vehicle-to-everything, composite term for both V2I and V2V
VBIED	vehicle borne improvised explosive device
WMD	weapons of mass destruction

EXECUTIVE SUMMARY

Terrorists throughout the world use vehicle borne improvised explosive devices (VBIEDs) to attack targets.[1] The availability of fully autonomous vehicles (FAVs) will change terrorism tactics by eliminating the need for martyrdom when delivering VBIEDs. As such, counter-terrorism forces must ask: What FAV technologies can be adapted to mitigate the threat of VIEBDs?

The future risk of explosives delivered by FAVs can be decreased by proactively implementing design and policy solutions today. Amplification of the current threat of (non-autonomous) VBIEDs can be gleaned by a comparison with small unmanned aircraft vehicles (UAVs). UAVs show how the seemingly benign availability of unmanned systems can easily be adapted as smart weapons for asymmetrical warfare.[2] This thesis overviews the projected threat posed by the nefarious use of FAVs as fully autonomous vehicle-borne improvised explosive devices (FAVBIEDs). This thesis shows how easily FAVs can be used for explosive delivery and discusses technological solutions that should be implemented, proactively, to reduce this threat. The overarching purpose of this thesis is also to capture what can be accomplished with public private partnerships working collaboratively to address strategic issues involving public safety in the United States.

Projecting and planning for devastating events or scenarios that have yet to occur is an ongoing challenge. More often than not, the first responder community reacts and adapts to unforeseen circumstances. The potential means by which a FAV can be weaponized are unsettlingly diverse. This research focuses on scenarios in which FAVs serve as VBIEDs that deliver their deadly cargo without occupants present. Imagination is a powerful tool. By drawing inspiration from prior appalling events and imagining

[1] Robert J. Bunker, "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials," TRENDS Research and Advisory, January 2016, http://trends institution.org/daeshis-armored-vehicle-borne-improvised-explosive-devices-avbieds-insurgent-use-and-terrorism-potentials/.

[2] Ryan Jokl Ball, *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications*, Technical Report No. LLNL-TR-740336 (Livermore, CA: Lawrence Livermore National Laboratory, 2017), 13, https://doi.org/10.2172/1410035.

them in an alternate setting via scenarios, it is the sincere desire of this author to impact the discussion on fully autonomous vehicle-borne improvised explosive device (FAVBIED) mitigating strategies positively.

Since the threat of terrorism to the U.S. homeland can be considered an uncontrollable external low occurrence risk, the intent of this thesis is not only to identify risks, but also acknowledge the potential impact and determine how to mitigate the effects if an event does occur.[3] To prioritize and assess risk, analysis should consider both the probability and consequences of a particular risk event. As this thesis explores the use of a technology that has yet to be commercially available to the general public, the probability of a FAVBIED is currently considered low. However, the consequences of a future successful deployment would be considerable.

With the development of the FAV in conjunction with the evolution of asymmetrical public safety threats, problems and solutions once inconceivable in past years are now commonplace and it can be expected that continued disruptive technologies will be dual-use when looking toward the future. Admittedly, without regulatory mandates for adoption, the incentive for FAV manufacturers to embrace and enact the proposed mitigating strategies is more a function of self-interest than altruism. Manufacture cost benefit analysis may indicate a course of action, or lack thereof, contrary to the best interests of public safety.

The development and implementation of FAVBIED mitigating strategies raises the prospect of synergistic opportunities amongst vehicle manufacturers and the homeland security enterprise while improving public safety and enhancing the overall transportation network experience. The following are specific recommendations:

- FAVs need to have constraints on where they are allowed to drive.
- FAVs need the ability to identity their users.

[3] Robert S. Kaplan and Anette Mikes, “Managing Risks: A New Framework,” *Harvard Business Review*, June 1, 2012, https://hbr.org/2012/06/managing-risks-a-new-framework.

- FAVs need internal capabilities to identity intended or unintended cargo or occupants.

- FAVs need internal and external system monitoring to identify unauthorized computer system access (aka hacking), a mechanism to report intrusions, and for the vehicle to have a back-up safety response default should systems be compromised.

- FAVs need the ability to receive and act upon instructions from external inputs, such as law enforcement or other public safety agencies.

The people of this great nation have an expectation they will be protected and it is the duty and moral obligation of this country as homeland security practitioners to engage proactively. An open and forthright policy discussion with transparent expectations needs to be established at the federal regulatory level. The current free-for-all "hands off" policy by government oversight agencies is understandable given the strategic importance of winning the race to full autonomy. Yet, to be fair, it is necessary to ask if this policy is contrary to public safety expectations.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This adventure would not have been accomplished without the unwavering encouragement and support of many different people. I work for an agency that promotes higher education and want specifically to thank Captain Dan Seaman for his patience and encouragement, which helped put me in a position to succeed. I also appreciate all those whom I work with who assisted me during this time.

Throughout the duration of this program, countless instructors contributed their wisdom as I grew in both the knowledge and capabilities that culminated with this thesis. Notably, I genuinely appreciate my thesis advisors, Robert Simeral and Dr. Tom Mackin, who were integral in helping me complete this daunting challenge.

I also want to recognize my parents and extended family, as they demonstrated by example the never-ending quest of being lifelong learners and the importance of pursuing higher education. Lastly, and most importantly, this thesis would not have been possible without the love and sacrifice of my wife, Lora, and daughters, Cheyenne and Shelby (who was looking down on me; smiling) because in the many late nights and times I would have rather been doing anything else other than working on my thesis, they understood and kept me focused.

Thank you all!

THIS PAGE INTENTIONALLY LEFT BLANK

Across the government, there were failures of imagination, policy, capabilities, and management. . . . The most important failure was one of imagination.

—The 9/11 Commission Report

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH QUESTION

What fully autonomous vehicle technologies can be adapted to mitigate the threat of vehicle borne improvised explosive devices (VBIEDs)?

B. PROBLEM STATEMENT

The evolution of vehicle technology is rapidly advancing and fully autonomous vehicles (FAVs) will be in use on U.S. streets, roads, and freeways in the foreseeable future.[1] These advancements will affect everyone, regardless of whether people are using one of these vehicles or simply reaping the ancillary benefits.[2] FAVs are projected to improve the standard of living for users and society as a whole by enhancing the efficiency of this country's transportation systems and reducing fatal and injury collisions.[3] However, the development of FAVs also has drawbacks. Even with good aims, new products and ideas can be re-purposed by people with bad intentions.

The Federal Bureau of Investigation (FBI) has already predicted, "bad actors will be able to conduct tasks that require use of either hands or taking one's eyes off the road which would be impossible today."[4] As an example, fleeing felons in FAVs could focus their attention on aggressively inhibiting pursuing law enforcement.[5] Another report generated within the FBI's Directorate of Intelligence relates, "Autonomy … will make mobility more efficient, but will also open up greater possibilities for dual-use

[1] Todd Litman, *Autonomous Vehicle Implementation Predictions Implications for Transport Planning* (Victoria, BC, Canada: Victoria Transport Policy Institute, 2017), 3, http://leempo.com/wp-content/uploads/2017/03/M09.pdf.

[2] James M. Anderson et al., *Autonomous Vehicle Technology: A Guide for Policymakers* (Santa Monica, CA: RAND, 2014), 9.

[3] Anderson et al., 15.

[4] Mark Harris, "FBI Warns Driverless Cars Could Be Used as 'Lethal Weapons,'" *The Guardian*, July 16, 2014, http://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous.

[5] Harris.

applications and ways for a car to be more of a potential lethal weapon than it is today."[6] Consideration should also be given to the prospect of FAVs being intentionally modified (hacked) so their safety protocols are circumvented to cause harm; or, it would even be easier to have a FAV transport cargo containing an improvised explosive device (IED).[7]

Terrorists throughout the world use VBIEDs, which makes them commonplace in the Middle East.[8] The availability of FAVs will change terrorism tactics, as the need for VBIED martyrdom operations decreases as the acquisition of FAVs becomes easier.

C. HYPOTHESIS

FAVs will be used to deliver IEDs in the future. "The concept of hazard mitigation begins with the realization that many disasters are not unexpected," as related by Bosher et al.[9] The future risk of explosive devices being delivered by FAVs can be decreased by considering design and policy solutions today. The current threat of (non-autonomous) VBIEDs has lessons to share. The parallels via increased accessibility of small unmanned aircraft vehicles (sUAVs) throughout the world also offer insight as these systems exemplify a dual-use technology easily adaptable for asymmetrical warfare.[10]

D. FOCUS AND GOAL

Projecting and planning for devastating events or scenarios that have yet to occur is an ongoing challenge for homeland security professionals. More often than not, the

[6] Harris.

[7] Harris.

[8] Robert J. Bunker, "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials," TRENDS Research and Advisory, January 2016, http://trendsinstitution.org/daeshis-armored-vehicle-borne-improvised-explosive-devices-avbieds-insurgent-use-and-terrorism-potentials/.

[9] Lee Bosher et al., "Built-in Resilience to Disasters: A Pre-emptive Approach," *Engineering, Construction and Architectural Management* 14, no. 5 (September 11, 2007): 434–46, https://doi.org/10.1108/09699980710780746.

[10] Ryan Jokl Ball, *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications*, Technical Report No. LLNL-TR-740336 (Livermore, CA: Lawrence Livermore National Laboratory, 2017), 13, https://doi.org/10.2172/1410035.

first responder community reacts and adapts to unforeseen circumstances. The potential means by which an autonomous vehicle can be weaponized are unsettlingly diverse. This research focuses on scenarios in which FAVs serve as VBIEDs that deliver their deadly cargo without occupants present. A "predictable is preventable" risk management approach is used as a part of the analysis.[11] Gordon Graham states, "Risk management is any activity that involves the evaluation of, or comparison of, risks and the development, selection and implementation of control measures that change outcomes."[12]

Keeping solutions simple will help to attain a balance between the desire to foster technological innovation and the desire to increase the likelihood of stakeholder buy-in and subsequent adoption. Proposed strategies look beyond considering only regulatory solutions requiring the development and integration of potentially expensive single-purpose hardware into FAVs. The goal of this thesis is to identify dual-use existing and projected technologies that, when adapted, will mitigate the threat of fully autonomous vehicle-borne improvised explosive devices (FAVBIEDs). Dual-use is the ability to leverage existing technology, including both hardware and software, to be used for a homeland security advantage.[13] A dual-use item, according to 15 CFR 730.3, "is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."[14] However, it should be noted that in an adversary's hands, dual-use may pose a risk and the *Long-range Emerging Threat Report to Congress* specifically identified unmanned vehicles as one of the examples.[15] Using this concept

[11] Gordon Graham, *Affairs of Government 2016: Some Thoughts on Real Risk Management* (Orem, UT: Utah Risk Management Mutual Association, 2016), 16, https://www.urmma.org/wp-content/uploads/2016/03/Gordon-Graham-2016-Handout.pdf; "6 Steps Risk Management Approach," *ECRRN European Cyber Resilience Research Network* (blog), March 9, 2016, https://www.ecrrn.com/blog/files/6b05d547c39af8ce6babd9e94b71fab0-4.html.

[12] Graham, 15.

[13] Clark McFadden and Dewey Ballantine, *International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings; Session 6—Dual-Use Technologies and National Security* (Washington, DC: The National Academies Press, 1997), 130–142, https://doi.org/10.17226/5902.

[14] "15 CFR 730.3—'Dual Use' and Other Types of Items Subject to the EAR," Cornell Law School, Legal Information Institute, accessed January 28, 2019, https://www.law.cornell.edu/cfr/text/15/730.3.

[15] Government Accountability Office, *Long-range Emerging Threats Facing the United States As Identified by Federal Agencies*, GAO-19-204SP (Washington, DC: Government Accountability Office, 2018), 6.

will make implementation of mitigating adaptations substantially more palatable to private industry autonomous vehicle developers.

E. RESEARCH CONTEXT

The focus on FAVBIEDs is simply to narrow down the topic of discussion as it is a projected threat. Discussions in Chapter II attempt to assist the reader in realizing the sizeable scope encompassing the multidimensional concerns with misusing this evolving FAV technology. Stakeholders for this topic include the automotive industry and ancillary developers, the homeland security enterprise with emphasis on local, state, and federal law enforcement, policy makers, businesses incorporating the use of FAVs, motorists, and the general public. There is a national strategic incentive to winning the FAV development race, as it will profoundly and positively impact American's way of life.[16] A nation that incorporates FAVs into its operational infrastructure will be able to reallocate previously utilized transportation resources (people) to other sectors and increase overall economic productivity; thereby, having a competitive advantage in the global economy.

The ongoing development of FAVs has not been without severe consequences. Deaths have already been attributed to FAVs being tested on public roadways.[17] Concerns about this technology rolling out too quickly at the expense of public safety are openly discussed and may slow down the pace of FAV development.[18] The threat of a FAVBIED is entirely realistic given VBIED experiences throughout the world. Simply put, hoping fully autonomous car bombs do not happen in the United States is not acceptable. As Anderson Cooper states, "Hope is not a plan."[19] The people of this great nation have an expectation they will be protected and it is this country's duty and moral

[16] Litman, *Autonomous Vehicle Implementation Predictions*, 9.

[17] Ed Garsten, "Sharp Growth in Autonomous Car Market Value Predicted but May Be Stalled by Rise in Consumer Fear," *Forbes*, August 13, 2018, https://www.forbes.com/sites/edgarsten/2018/08/13/sharp-growth-in-autonomous-car-market-value-predicted-but-may-be-stalled-by-rise-in-consumer-fear/.

[18] Garsten.

[19] Roxanne Parrott, "How Does Anderson Cooper's Statement, 'Hope Is Not a Plan' Fit Today's Events?," *Talking about Health; Why Health Communication Matters* (blog), August 8, 2011, http://whyhealthcommunication.com/whc_blog/2011/08/08/how-does-anderson-coopers-statement-hope-is-not-a-plan-fit-todays-events/.

obligation as homeland security practitioners to engage proactively. This thesis is intended to cause pause and articulate the need for FAV development to incorporate FAVBIED mitigating strategies actively.

F. LITERATURE REVIEW

Viewing threats concerning the weaponization of FAVs as self-guided IEDs have many facets. Research includes reviewing the current use of VBIED both in the U.S. homeland and overseas. Parallel and evolving technologies, such as unmanned aerial vehicles (UAV) offer many lessons learned for this nation to extrapolate their threat potential to FAVs. Also, thought needs to be given to autonomous vehicle operating parameters based on their development, susceptibility, and current regulatory environment within the United States

1. Fully Autonomous Vehicle Overview

FAVs are on the cusp of becoming accessible to the masses and are already being tested in public environments throughout the United States. Lewis, Rodgers, and Turner state, "governments are under pressure to craft regulations and make investments that encourage innovation while still enhancing safety and protecting the public interest."[20] The different levels of vehicle automation are explored along with FAV technologies and government regulation. The technologies in FAVs will have the likely benefit of reducing the amount of American lives lost each year by preventing most traffic collisions involving human error.[21] At the same time, FAVs will be susceptible to those with bad intentions and can be made into devastating weapons.[22] Having a basic understanding of these FAV topics assists the reader with understanding the premise of FAVBIEDs and their threat to homeland security.

[20] Paul Lewis, Gregory Rogers, and Stanford Turner, *Beyond Speculation Automated Vehicles and Public Policy—An Action Plan for Federal, State, and Local Policymakers* (Washington, DC: Eno Center for Transportation, 2017), 1, https://www.enotrans.org/wp-content/uploads/2017/04/AV_FINAL-1.pdf?x43122.

[21] Anderson et al., *Autonomous Vehicle Technology*, 4.

[22] David R. Baker, "How Self-Driving Cars Could Become Weapons of Terror," *San Francisco Chronicle*, updated October 11, 2016, http://www.sfchronicle.com/business/article/How-self-driving-cars-could-become-weapons-of-9958541.php.

Understanding FAVs requires some general knowledge regarding the nuanced levels of automation. The *Federal Automated Vehicles Policy* states, "An automated vehicle system is a combination of hardware and software (both remote and on-board) that performs a driving function, with or without a human actively monitoring the driving environment."[23] The commonly accepted FAV taxonomy is via the Society of Automotive Engineers (SAE) International classifications, which has definitions for six levels, as shown in Figure 1.[24] SAE levels for vehicles are relative to "who does what, when."[25] Of note is the alternative taxonomy by the National Highway Traffic Safety Administration (NHTSA) which uses five levels; however, with both scales the highest level of automation in each of the systems is fully autonomous.[26] The SAE system has more industry acceptance as opposed to the NHTSA standard, which can still be referenced in government-generated documents.[27]

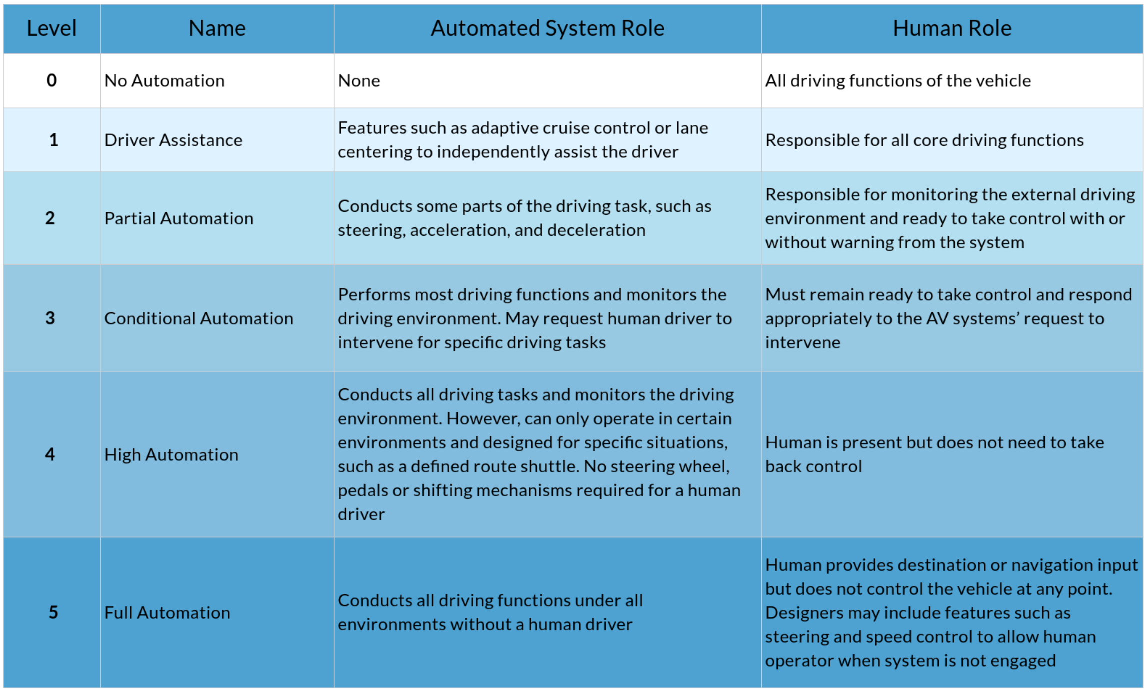
[23] National Highway Transportation Safety Agency, *Federal Automated Vehicles Policy—Accelerating the Next Revolution in Roadway Safety* (Washington, DC: Department of Transportation, 2016), 10, https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.

[24] National Highway Transportation Safety Agency, 9.

[25] National Highway Transportation Safety Agency, 9.

[26] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *Future Environmental Net Assessment: Autonomous Vehicles* (Washington, DC: Department of Homeland Security, 2017), 2.

[27] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, 2.



Level	Name	Automated System Role	Human Role
0	No Automation	None	All driving functions of the vehicle
1	Driver Assistance	Features such as adaptive cruise control or lane centering to independently assist the driver	Responsible for all core driving functions
2	Partial Automation	Conducts some parts of the driving task, such as steering, acceleration, and deceleration	Responsible for monitoring the external driving environment and ready to take control with or without warning from the system
3	Conditional Automation	Performs most driving functions and monitors the driving environment. May request human driver to intervene for specific driving tasks	Must remain ready to take control and respond appropriately to the AV systems' request to intervene
4	High Automation	Conducts all driving tasks and monitors the driving environment. However, can only operate in certain environments and designed for specific situations, such as a defined route shuttle. No steering wheel, pedals or shifting mechanisms required for a human driver	Human is present but does not need to take back control
5	Full Automation	Conducts all driving functions under all environments without a human driver	Human provides destination or navigation input but does not control the vehicle at any point. Designers may include features such as steering and speed control to allow human operator when system is not engaged

Source: Adapted from SAE Levels of Automation

Created by: Ann Henebery / Eno Center for Transportation

Figure 1. SAE Classification System for Vehicle Levels of Automation[28]

Current mass produced vehicles available for public purchase already contain features that automate driving tasks.[29] Vehicles rated as Level 1 are readily available. There are some luxury vehicle manufacturers, including Cadillac, Mercedes, Lexus, and Tesla, that incorporate Level 2 features.[30] Lewis et al. identifies several current vehicle features that can be considered Level 2 including adaptive cruise control, lane centering systems, preemptive braking systems, parking assist systems, driver monitoring technology and combining automated features that will brake, accelerate and steer on a specified roadway while being monitored by a driver.[31] Level 1 and Level 2 vehicles both require active driver attention as opposed to higher levels.

[28] Source: Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 4.

[29] Michael Casey, "Want a Self-Driving Car? Look on the Driveway," *Fortune*, December 6, 2014, http://fortune.com/2014/12/06/autonomous-vehicle-revolution/.

[30] Andrew Silver, "Autonomous Technology May Encourage a False Sense of Security," Trucker, September 10, 2017, http://trucker.com/technology/autonomous-technology-may-encourage-false-sense-security.

[31] Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 4.

Challenges are associated with developing and implementing more advanced levels of automation. For instance, Lewis et al. relate, "In Level 3, the vehicle's driving system is monitoring the environment, but if it detects a scenario that it cannot navigate, it warns the human driver and control is transferred back to the human."[32] One of the problems with having a Level 3 vehicle transfer control back would be having a driver re-acclimate to the circumstance that could take up to 17 seconds.[33] Even with the possibility that current Level 2 automation may provide a false sense of security, these systems perform quite well and are even safer than current human drivers.[34] Of note is Tesla's self-driving technology, which has been credited with reducing crashes with their vehicles by almost 40%.[35] In fact, Tesla vehicles traveled over 130 million miles before attaining their first fatality compared to the fatality rate of human drivers, which is one every approximately 94 million miles.[36] Unlike Tesla, both Ford Motor Corporation and Google (Waymo) have indicated they intend to forego Level 3 driver assistance systems and focus on implementing FAVs that require no human intervention.[37] The difference in a manufacturer's approach to attaining full autonomy is interesting as, for example, Tesla appears to have a more incremental approach as opposed to Waymo, which appears to be intent on hitting the proverbial homerun.

Different overarching concepts state how vehicles will obtain fully autonomous capabilities. Vehicle-to-infrastructure (V2I) demonstration systems have already been built and successfully used as far back as 1991 in San Diego.[38] Vehicle-to-vehicle (V2V)

[32] Lewis, Rogers, and Turner, 11.

[33] Paul Lienert and Joseph White, "Automakers, Google Take Different Roads to Automated Cars," *Reuters*, September 4, 2015, https://www.reuters.com/article/us-autos-selfdriving-gurus-insight-idUSKCN0R40BX20150904.

[34] Tom Randall, "Tesla's Autopilot Vindicated with 40% Drop in Crashes," *Bloomberg*, January 19, 2017, https://www.bloomberg.com/news/articles/2017-01-19/tesla-s-autopilot-vindicated-with-40-percent-drop-in-crashes.

[35] Randall.

[36] Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 11.

[37] Neal E. Boudette, "Big Carmakers Merge, Cautiously, Into Self-Driving Lane," *New York Times*, September 2, 2016, late edition, sec. B.

[38] Matt Novak, "The National Automated Highway System that Almost Was," *Smithsonian*, May 16, 2013, https://www.smithsonianmag.com/history/the-national-automated-highway-system-that-almost-was-63027245/.

communications allow for the sharing of vehicle sensor data in a network capacity.[39] Both V2I and V2V capabilities can be referred to as V2X (vehicle-to-everything).[40] As Canis states:

> V2X technology relies on communication of information to warn drivers about dangerous situations that could lead to a crash, using dedicated short-range communication to exchange messages about vehicles' speeds, braking status, stopped vehicles ahead, or blind spots to warn drivers so they can take evasive action… within a range of 300 meters... up to twice the distance of onboard sensors.[41]

Leveraging V2X communications will help the entire transportation network via collision avoidance, minimizing congestion, and benefiting the environment.[42] Caution should be exercised, as when these networks become integrated into the U.S. transportation architecture, they may be susceptible to cyber vulnerabilities and be subjected to large-scale attacks with large-scale consequences.[43]

Current FAVs are considered "smart vehicles," as they operate without the requirement for special infrastructure or outside input; they are self-contained.[44] Smart vehicles use different kinds of electronic sensors in various combinations in an effort to achieve autonomous driving. *Future Environment Net Assessment* also relates, "The majority of autonomous vehicles in development use a deliberative architecture, meaning they are capable of making decision entirely based on onboard technology—though many are also capable of incorporating external inputs."[45] With no standardized sensor package

[39] Jean Yoder, "Vehicle-to-Vehicle Communication," National Highway Transportation Safety Agency, October 26, 2016, https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication.

[40] Brett Berk, "We Hack a Car (It's Way Easier than You Might Think)," *Automobile Magazine* (blog), January 11, 2019, https://www.automobilemag.com/news/car-hacking-we-hack-autonomous-car/?sc_cid=AppleNewsAMAGArticle.

[41] Yoder, "Vehicle-to-Vehicle Communication."

[42] Yoder.

[43] Philip Barnes and Eli Turkel, *Autonomous Vehicles in Delaware: Analyzing the Impact and Readiness for the First State* (Newark, DE: Institute for Public Administration, School of Public Policy and Administration, University of Delaware, 2017), 14.

[44] Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 6.

[45] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *Future Environmental Net Assessment*, 1.

configuration being used, FAV manufacturers are incorporating different strategies to achieve automation, as demonstrated in Figure 2.

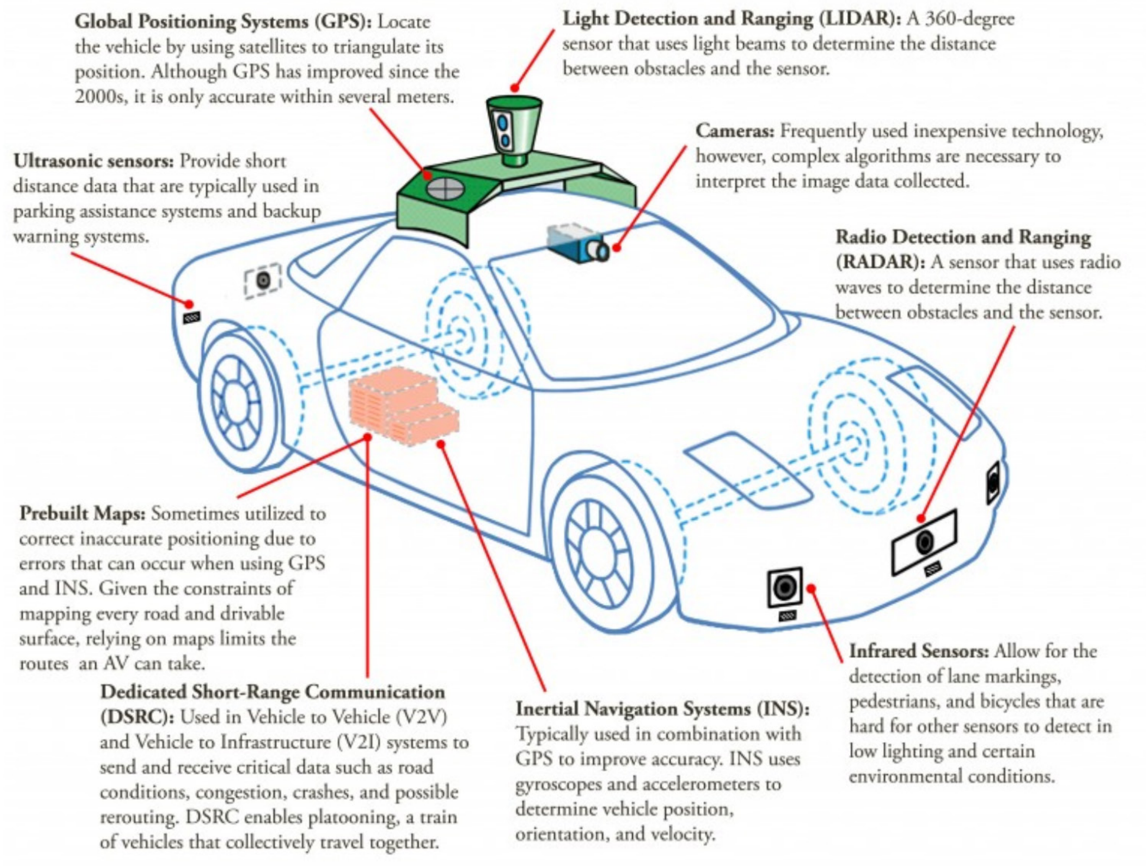

Global Positioning Systems (GPS): Locate the vehicle by using satellites to triangulate its position. Although GPS has improved since the 2000s, it is only accurate within several meters.
Light Detection and Ranging (LIDAR): A 360-degree sensor that uses light beams to determine the distance between obstacles and the sensor.
Cameras: Frequently used inexpensive technology, however, complex algorithms are necessary to interpret the image data collected.
Ultrasonic sensors: Provide short distance data that are typically used in parking assistance systems and backup warning systems.
Radio Detection and Ranging (RADAR): A sensor that uses radio waves to determine the distance between obstacles and the sensor.
Prebuilt Maps: Sometimes utilized to correct inaccurate positioning due to errors that can occur when using GPS and INS. Given the constraints of mapping every road and drivable surface, relying on maps limits the routes an AV can take.
Dedicated Short-Range Communication (DSRC): Used in Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) systems to send and receive critical data such as road conditions, congestion, crashes, and possible rerouting. DSRC enables platooning, a train of vehicles that collectively travel together.
Inertial Navigation Systems (INS): Typically used in combination with GPS to improve accuracy. INS uses gyroscopes and accelerometers to determine vehicle position, orientation, and velocity.
Infrared Sensors: Allow for the detection of lane markings, pedestrians, and bicycles that are hard for other sensors to detect in low lighting and certain environmental conditions.

Figure 2. Autonomous Vehicle Technologies[46]

Connected FAVs will be integrated with huge volumes of data, and subsequently, demand vigorous cybersecurity attention.[47] Many different stakeholders would desire access to the data FAVs collect including, but not limited to the law enforcement and first responder community, vehicle manufacturers, vehicle owners, other various state, federal and local governmental agencies, academic institutions, corporations that use analytics to

[46] Source: Center for Sustainable Systems, *Autonomous Vehicles Factsheets Mobility* (Ann Arbor, MI: University of Michigan, 2018), 1, http://css.umich.edu/sites/default/files/Autonomous_Vehicles_Factsheet_CSS16-18_e2018_0.pdf.

[47] Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 1.

develop user profiles for commercial purposes, and a host of other interest groups, some of which have yet to be conceived.[48] Consideration needs to be given as to who has access to FAV data and a host of user privacy issues that are beyond the scope of this thesis.

A current day example involves currently available vehicles. These vehicles already have a mechanism to maintain a record of basic operational information in a standardized format via an event data recorder (EDR), also known as a "black box."[49] Mechanisms are in place concerning how EDR information can be legally accessed via a court order or consent.[50] Data access for FAV manufacturers is easily above and beyond what would traditionally be retained for the purposes of an EDR. Data ownership is already a concern, as FAV manufacturers currently access and use accumulated vehicle data to improve product capabilities.[51]

FAV software will need to be secured, as those with nefarious intentions may illegally access it and cause harm, also known as "hacking." Current vehicles are already susceptible to hacking, as seen in Figure 3. System security weaknesses have been exploited, as demonstrated with different examples including the Jeep Cherokee, Toyota Prius, Ford Escape, and Chevy Corvette.[52] Industry has attempted to counter this threat through sharing information on vulnerabilities and cyber threats via the Automotive Information Sharing and Analysis Center non-profit organization.[53] NHTSA has also

[48] Lewis, Rogers, and Turner, 14.

[49] Lewis, Rogers, and Turner, 15.

[50] Brent R. Cooper, "Event Data Recorders: Balancing the Benefits and Drawbacks," IRMI, August 2008, https://www.irmi.com/articles/expert-commentary/event-data-recorders-balancing-the-benefits-and-drawbacks.

[51] Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 15.

[52] Andy Greenberg, "Securing Driverless Cars from Hackers Is Hard. Ask the Ex-Uber Guy Who Protects Them," WIRED, April 12, 2017, https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

[53] Alliance of Automobile Manufacturers, "Automotive Industry Collaborates in Developing Vehicle Cybersecurity Best Practices to Address Cybersecurity Challenges," CISION PR Newswire, July 21, 2016, https://www.prnewswire.com/news-releases/automotive-industry-collaborates-in-developing-vehicle-cyber security-best-practices-to-address-cybersecurity-challenges-300301805.html.

provided "guidance" for cybersecurity best practices.[54] Of note is the aforementioned guidance is *voluntary*, and for example, does not specify what acceptable levels of cybersecurity are.[55] Ultimately, as evolving technologies are increasingly present in FAVs, a rise in cyber risk should be expected.[56] Private industry has shown a proclivity to be slow in resolving cybersecurity issues and manufacturers appear to have not possibly taken this issue seriously, which leads to the topic of government regulation.[57]

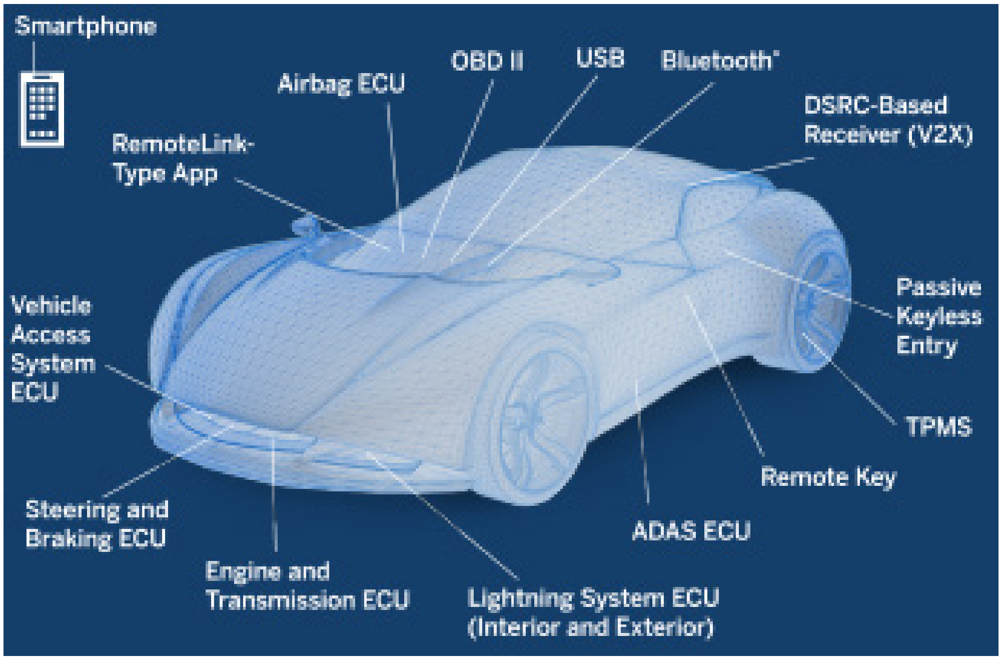


Figure 3. Fifteen of the Most Hackable and Exposed Attack Surfaces on a Next-generation Car[58]

[54] National Highway Traffic Safety Administration, *Cybersecurity Best Practices for Modern Vehicles* (Washington, DC: National Highway Traffic Safety Administration, 2016), 5, https://www.nhtsa.gov/static files/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[55] Baker, "How Self-Driving Cars Could Become Weapons of Terror."

[56] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *Future Environmental Net Assessment*, 6.

[57] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, 7.

[58] Source: "Car of the Future, Trends in Next-Generation Automotive Safety and Security," *Intel* 1 (Winter 2017): 2.

Regulators and lawmakers are wary of constraining automakers and technology companies with rules that may potentially inhibit innovation. However, a need also exists to balance governmental oversight with concerns held by safety advocates who worry FAVs may be made available to the public without the necessary research and development (R&D). For FAV technology to be certified by the NHTSA, manufacturers will need to demonstrate their vehicles are safer than those being driven by humans for the certified driving environment, as seen in Figure 4.[59] Fraade-Blanar and Kalra discuss current FAV safety performance can only be proven in real-time by measuring the propensity of negative outcomes, such as collisions.[60] Parallels for the adoption of new FAV technology can be drawn from the pharmaceutical industry when Eichler et al. relate government officials and manufacturers need to recognize constraints are placed on resources and an unwillingness exists to accept safety risk, aka uncertainty, that may be potentially measured in lives lost, as the opportunity cost of delaying product availability may be worse than not making the product available in the first place.[61] FAVs, according to Fraade-Blanar and Kalra will, "likely improve in safety and function as they are exposed to more environments due to machine-based learning methods."[62] The converse also needs to be acknowledged, as stated by Jacqueline Gillian, President of Advocates for Highway and Auto Safety, who states, "policy and legal gaps could result in consumers becoming 'human crash test dummies'… we welcome innovation and the life-saving potential of AVs, we are concerned about life-threatening dangers in a rush to market."[63]

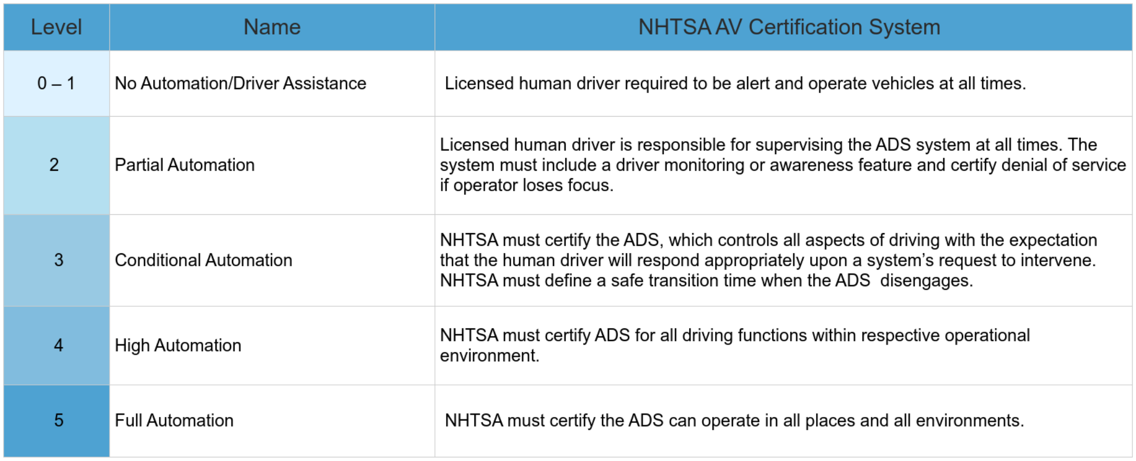
[59] Randall, "Tesla's Autopilot Vindicated with 40% Drop in Crashes."

[60] Laura Fraade-Blanar and Nidhi Kalra, *Autonomous Vehicles and Federal Safety Standards: An Exemption to the Rule?* (Santa Monica, CA: RAND, 2017), 5.

[61] Fraade-Blanar and Kalra, 5.

[62] Fraade-Blanar and Kalra, 6.

[63] "Statement of Jackie Gillan on DOT Release of Federal AV Policy," *Advocates for Highway and Auto Safety* (blog), September 20, 2016, https://saferoads.org/2016/09/20/statement-of-jackie-gillan-on-dot-release-of-federal-av-policy/.



Level	Name	NHTSA AV Certification System
0 – 1	No Automation/Driver Assistance	Licensed human driver required to be alert and operate vehicles at all times.
2	Partial Automation	Licensed human driver is responsible for supervising the ADS system at all times. The system must include a driver monitoring or awareness feature and certify denial of service if operator loses focus.
3	Conditional Automation	NHTSA must certify the ADS, which controls all aspects of driving with the expectation that the human driver will respond appropriately upon a system's request to intervene. NHTSA must define a safe transition time when the ADS disengages.
4	High Automation	NHTSA must certify ADS for all driving functions within respective operational environment.
5	Full Automation	NHTSA must certify the ADS can operate in all places and all environments.

Created by: Ann Henebery / Eno Center for Transportation

Figure 4. Certification Levels for Automated Driving Systems (ADS)[64]

The advent of FAV capabilities is putting government regulators in an unenviable position. The federal government is slowly attempting to take the legislative lead. An overarching concern for the FAV industry is the patchwork of regulations from federal, state, and local jurisdictions that have the potential to inhibit testing and sales.[65] Different federal documents have been generated, such as *Vehicle Performance Guidance*, which provides a best practices list for the safe design and testing for the pre-deployment of FAVs and "asks" manufactures submit a safety assessment letter.[66] The U.S. Department of Transportation also developed a *Model State Policy*, which, "confirms that States retain their traditional responsibilities for vehicle licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability."[67] Actions by the federal government are not necessarily matching their rhetoric as NHTSA administrator Mark Rosekind does not want to impede the push for life saving technologies as a result of a

[64] Source: Lewis, Rogers, and Turner, *Beyond Speculation Automated Vehicles and Public Policy*, 13.

[65] Michaela Ross, "Thune, Peters Eye Self-Driving Car Bill," Bloomberg Law, BNA, February 15, 2017, https://www.bna.com/thune-peters-eye-n57982083844/.

[66] Department of Transportation, *AV Fact Sheet—Vehicle Performance Guidance* (Washington, DC: Department of Transportation, 2016), 1, https://www.transportation.gov/AV/av-fact-sheet-vehicle-performance-guidance.

[67] Department of Transportation, *AV Fact Sheet—Model State Policy* (Washington, DC: Department of Transportation, 2016), 1, https://www.transportation.gov/AV/av-fact-sheet-model-state-policy.

single incident (i.e., the Tesla fatal collision).[68] However, at the same time, the NHTSA has no published regulations for the development of FAVs, as stated by Kelley, "leaving a vacuum that state legislatures and industry lobbyists are rushing to fill with conflicting laws and regulations."[69] Figure 5 shows which states have enacted autonomous vehicle legislation and executive orders. Joan Claybrook, former NHTSA administrator, warned, "If there are no rules for adequately testing self-driving technology before it becomes a highway reality, motorists like the driver in the fatal Tesla 'autopilot' crash will become unwitting guinea pigs in the trial-and-error evolution of automated vehicles."[70] From an evaluative perspective relative to the international FAV developmental environment, KPMG Infrastructure Advisor Timothy Wilschetz states:

> The U.S. has a highly innovative but largely disparate environment with little predictability regarding the uniform adoption of national standards for AVs. Therefore, the prospect of widespread driverless vehicles is unlikely in the near future. However, federal policy and regulatory guidance could certainly accelerate early adoption, particularly concerning limited freight applications such as truck platooning.[71]

Simply put, historical approaches to automobile manufacturer safety regulations are not capable of keeping up with these rapidly developing FAV technologies.

[68] Ben Kelley, "Miles to Go on Highway Safety," *FairWarning.Org* (blog), September 7, 2016, https://www.fairwarning.org/2016/09/miles-go-highway-safety/.

[69] Kelley.

[70] Kelley.

[71] Richard Threlfall, *Autonomous Vehicles Readiness Index* (Amstelveen, Netherlands: KPMG International, 2018), 17.

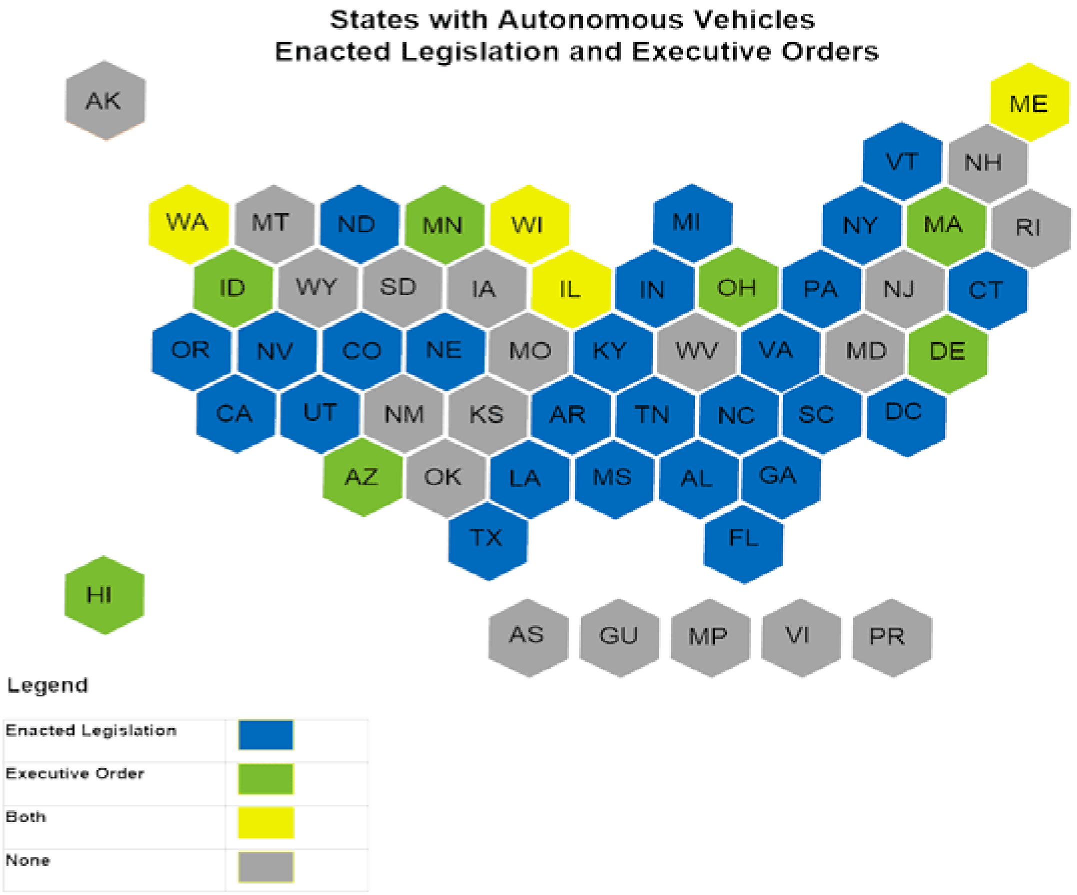


Figure 5. States with Enacted Autonomous Vehicle Legislation and Executive Orders[72]

Many projected positive outcomes and areas of concern are associated with the deployment of FAVs in the United States. FAVs have an incredible potential to reduce both annual fatalities and injury collisions on American roadways, which are estimated to be approximately 40,000 and 4.57 million, respectively.[73] Approximately 94% of fatal and injury collisions are attributed to human error.[74] Further, reducing costs associated with fatal and injury collisions could result in projected governmental savings in the

[72] Source: "Autonomous Vehicles|Self-Driving Vehicles Enacted Legislation," National Conference of State Legislatures, November 7, 2018, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#Enacted%20Autonomous%20Vehicle%20Legislation.

[73] National Safety Council, *NSC Motor Vehicle Fatality Estimates* (Itasca, IL: National Safety Council, 2017), 1, https://www.nsc.org/portals/0/documents/newsdocuments/2018/december_2017.pdf.

[74] Michael Clamann, Miles Aubert, and Mary L. Cummings, *Evaluation of Vehicle-to-Pedestrian Communication Displays for Autonomous Vehicles* (Berlin, Germany: ResearchGate, 2017), 3.

neighborhood of $10 billion annually.[75] The current limited deployment of FAVs has indicated where safety benefits can be gained, but their true life-saving value will only be realized once FAVs are deployed on a large scale.[76] If U.S. FAV industries are to remain relevant and garner a competitive advantage for future generations this nation needs to embrace non-traditional certification methodologies for FAVs and even then uncertainty will persist.[77] Current governmental oversight with a "hands off" approach can be a cause for concern and states are responding with piecemeal legislation that can cause long-term FAV development challenges. Cyber vulnerabilities are a threat, yet they are not the only FAV fear. As stated by Dubno et al., "It would not require 'hacking' of an autonomous vehicle to cause a profound terror attack."[78]

2. Vehicle Borne Improvised Explosive Device Threats

The car bomb is the nuclear weapon of guerrilla warfare.

—Washington Post columnist, Charles Krauthammer[79]

The threat of VBIEDs exists throughout the world, including the United States. This section considers the evolution of this threat, the increasing use of VBIEDs, and lays a foundation for threat assessment in which this weapon of terror may incorporate the use of FAVs. Different aspects of VBIEDs are discussed in this portion of the literature review. The National Science and Technology Council, Domestic Improvised Explosive Devices Subcommittee (DIEDS), related:

[75] Kevin C. Fedorschak and Kena Fedorschak, "Autonomous Vehicles Will Have Tremendous Impacts on Government Revenue," *Brookings* (blog), July 7, 2015, https://www.brookings.edu/blog/techtank/2015/07/07/autonomous-vehicles-will-have-tremendous-impacts-on-government-revenue/.

[76] Fraade-Blanar and Kalra, *Autonomous Vehicles and Federal Safety Standards*, 1.

[77] Nidhi Kalra and Susan M. Paddock, "Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?," *Transportation Research Part A: Policy and Practice* 94 (2016): 1.

[78] Daniel Dubno et al., "Autonomous Technology White Paper, Homeland Security Science and Technology Advisory Committee (HSSTAC) Quadrennial Homeland Security Review Subcommittee," *Homeland Security, Science and Technology*, March 10, 2017, 4.

[79] Mike Davis, "Car Bombs with Wings: A History of the Car Bomb (Part 2)," TomDispatch, April 13, 2006, http://www.tomdispatch.com/post/76824/.

> The threat of explosives attacks in the United States is of great concern considering terrorists' demonstrated ability to make, obtain, and use explosives; the ready availability of Components used in the construction of Improvised Explosive Devices (IEDs); the relative technological ease with which an IED can be fashioned; and the nature of our free society.[80]

A VBIED, according to Kaaman, is considered a vehicle, "altered so as to sole function as a large rolling IED."[81] VBIEDs can be parked at a target location and be detonated by a timer or remotely, or they can be used by a suicide bomber and driven upon the target location.[82] VBIEDs are a weapon of choice for terrorists.

DIEDS analysis of terrorist intelligence pursuant to global events and past experience suggests the high probability VBIEDs will be used to attack this nation.[83] The DIEDS state:

> Factors contributing to the popularity of VBIEDs among terrorists are the wide availability of materials used to make IEDs; the ability to conceal large amounts of explosives; the ease of getting the vehicle to the target; the proliferation of bomb-making instructions; and a history of extensive experience and success, which increases repetition and imitation.[84]

Kaaman relates inferior forces can use VBIEDs in martyrdom operations that are technologically inferior and smaller in size to strike their enemies accurately.[85] DIEDS relates, "Improvised explosive devices are not the product of logic, but of evolution; an inelegant process. Bomb makers do not choose the logically best design to meet their needs; they adapt what already exists."[86] Terrorists tend to favor weapons based on access and familiarity; thus, they go with what they know.

[80] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States* (Washington, DC: National Science and Technology Council, 2008), 9.

[81] Hugo Kaaman, "The Evolution of Suicide Car Bombs Examined," Action on Armed Violence, August 23, 2017, https://aoav.org.uk/2017/evolution-suicide-car-bombs/.

[82] Kaaman.

[83] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 14.

[84] Subcommittee on Domestic Improvised Explosive Devices, 18.

[85] Kaaman, "The Evolution of Suicide Car Bombs Examined."

[86] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 26.

VBIEDs, from a terrorist perspective, are a great *bang for your buck.* The Provisional Irish Republican Army (IRA) is attributed with improvising one of the first car bombs to use ammonium nitrate-fuel oil (ANFO), which are incredibly powerful and inexpensive to fabricate.[87] Davis relates, "the car bomb is the quotidian workhorse of urban terrorism."[88] VBIEDs are extraordinarily cheap and require only fertilizer, a vehicle, and minimal electronics.[89] As an example, the 1993 World Trade Center VBIED attack cost approximately $3,615 for one half ton of urea and $59 a day rental for the Ryder van.[90] Davis further relates that VBIEDs are operationally simple to organize as demonstrated by McVeigh and Nichols who, "successfully planned and executed the horrendous Oklahoma City bombing with instructional books and information acquired from the gun-show-circuit."[91] The threat of VBIEDs will remain, in part, due to their simplicity and accessibility, as well as being hard to stop.

Detecting and defeating VBIEDs is a formidable challenge. VBIEDs are, as stated by Lewis, "very difficult to anticipate and intercept."[92] As VBIEDs are frequently built by using local resources, they are very challenging to detect simply by observation, as they blend in with their surroundings.[93] Specifically, the DIEDS identified many operational needs including vehicle-borne IED detection.[94] Many challenges are associated with the detection and defeat of VBIEDs. DIEDS states, "No existing solutions provide the ability to detect a VBIED, with any reasonable degree of assurance, at a sufficient distance, and in sufficient time, to allow actions to be taken to safely deal

[87] Mike Davis, "Poor Man's Air Force, A History of the Car Bomb," *Coldtype.Net*, 2006, 5.

[88] Davis, 7.

[89] Davis, 7.

[90] Davis, 7.

[91] Davis, 7.

[92] Jeffrey William Lewis, "The Human Use of Human Beings: Suicide Bombing, Technological Innovation, and the Asymmetry of Modern Warfare," *Global Politics Review* 2, no. 2 (October 2016): 17.

[93] Joint Counterterrorism Assessment Team, *VBIED-Preparedness-Recognition-Response-ONLINE-Version* (Washington, DC: Office of the Director of National Intelligence, 2018), 1, https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/VBIED-Preparedness-Recognition-Response-ONLINE-Version.pdf.

[94] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 11.

with the threat posed by that device."[95] Challenges include almost any vehicle can be used as a VBIED, no explicit explosive is associated with VBIEDs, existing technologies have high false alarm rates, low through rates occur at vehicle detection locations, vehicle concealment areas are difficult to penetrate with detection equipment, depending on the detection equipment passengers may have to disembark the vehicle, and detection technology may be costly to purchase, maintain, and operate.[96] VBIEDs are stealth weapons of destructive efficiency, as they can easily transport their weaponized cargo to an opportunistic target.[97] As the size of a VBIED can vary from a few pounds of explosives to thousands of pounds of explosives with different bomb configurations, bomb technician safety is of paramount concern for render-safe operations.[98] Technicians will need access to a wide range of tools and technologies when attempting to defeat VBIEDs.[99] A study of VBIED rammings into transportation infrastructure noted the attacks utilized automobiles, motorcycles, and even a bicycle.[100] VBIEDs are also challenging, as they are highly anonymous and very little forensic evidence will be available post incident.[101] Further, as related by the Joint Counterterrorism Assessment Team (JCAT), "A VBIED attack can rapidly deplete first responder resources, tax command structures, and overwhelm emergency medical services."[102] Given the aforementioned detection and defeat challenges, it is also necessary to understand the different types of VBIEDs.

[95] Subcommittee on Domestic Improvised Explosive Devices, 18.

[96] Subcommittee on Domestic Improvised Explosive Devices, 19.

[97] Davis, "Poor Man's Air Force," 7.

[98] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 22.

[99] Subcommittee on Domestic Improvised Explosive Devices, 22.

[100] Brian Michael Jenkins and Bruce R. Butterworth, *Terrorist Vehicle Attacks on Public Surface Transportation Targets* (San Jose, CA: Mineta Transportation Institute, San Jose State University, 2017), 5, http://transweb.sjsu.edu/sites/default/files/terrorist-vehicle-attacks-on-public-surface-transportation-targets_0.pdf.

[101] Davis, "Poor Man's Air Force," 7.

[102] Joint Counterterrorism Assessment Team, *VBIED-Preparedness-Recognition-Response-ONLINE-Version*, 2.

VBIED are categorized differently. Parked VBIEDs when the driver escapes can generally be referred to as *static* for which Bunker classifies as Type 1. Suicide VBIEDs (SVBIED) can be divided into two main categories, referred to by Kaaman as covert and up-armored.[103] Civilian vehicles driven by a martyr carrying hidden explosives are considered covert.[104] Bunker refers to covert suicide vehicles as Type 2, which is a mobile variant of an unarmored Type 1.[105] In Bunker typology, the newest iteration is a Type 3 variant, which is an up-armored Type 2; also referred to as a "Mad Max," "hillbilly," "Franken-trucks," or "heavy VBIEDs."[106] Up-armored means a vehicle has metal plates attached that offer defensive capabilities to protect the driver and cargo from attack. Type 3 VBIEDs have also transitioned to include not just up-armored cars, but captured military vehicles, construction equipment, and different kinds of commercial or industrial vehicles.[107] Static VBIEDs, Type 1, are more associated with insurgency tactics as opposed to Type 2 and Type 3 suicide VBIEDs, which are more suited for offensive tactics that mainly engage well-defended targets.[108] Kaaman described the tactical shift by the Islamic State in Syria and Iraq during 2013 and 2014 stating, "The switched to almost entirely using up-armored SVBIEDs in areas that they swept through, a change necessitated by the shift away from guerrilla tactics to more semi-conventional combat in these areas."[109] The next evolution of VBIEDs may very well incorporate a variant whereby the vehicle has a driverless capacity as referenced in a Daesh "jihadi university video" where a martyr is no longer needed.[110] Given the tactical evolution of VBIEDs,

[103] Kaaman, "The Evolution of Suicide Car Bombs Examined."

[104] Kaaman.

[105] Bunker, "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs)."

[106] Bunker.

[107] "ISIS Releases Photos of Militants Using U.S. M113s as VBIEDS," Military.com, October 30, 2014, https://www.military.com/defensetech/2014/10/30/isis-releases-photos-of-militants-using-u-s-m113s-as-vbieds.

[108] Kaaman, "The Evolution of Suicide Car Bombs Examined."

[109] Kaaman.

[110] Stuart Ramsay, "Exclusive: Inside IS Terror Weapons Lab," Sky News, January 5, 2016, https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883.

consideration should be given to historical perspectives that can assist with understanding the threat to the U.S. homeland.

VBIEDs have been successfully used throughout the world by many different terrorist organizations. The first prototype car bomb was a wagon loaded with stolen dynamite and scrap metal in 1920.[111] Anarchist Mario Buda's explosion on Wall Street resulted in over 200 wounded and 40 deaths, including the horse, which demonstrates the ability to bring an inconspicuous vehicle transporting large amounts of explosives in the immediate proximity of a high-value target.[112] VBIEDs were revisited in the 1940s in Palestine by the Stern Gang, a pro-fascist splinter group, and used sporadically throughout the world until the 1970s.[113] The IRA used a notable concentration of VBIEDs in the 1970s through the 1990s in both England and Northern Ireland.[114] Literature agrees that Hezbollah's innovative use of VBIEDs in Lebanon during the 1980s was successful at countering the military technology of major countries including the United States, France, and Israel.[115] These attacks forced both France and the United States out of Lebanon.[116] President Ronald Reagan stated in *An American Life*:

> The price we had to pay in Beirut was so great, the tragedy at the barracks was so enormous… We had to pull out… We couldn't stay there and run the risk of another suicide attack on the Marines. No one wanted to commit our troops to a full-scale war in the Middle East.[117]

Suicide bombings, which include VBIEDs, are now a major alternative technological strategy that contributes to asymmetric combat where minimally funded adversaries challenge well-funded nation states. Lewis states, "Suicide bombers are thus representative of a trend in the development of technology by non-state actors such as guerrilla and terrorist groups—the development of simple, robust, and inexpensive

[111] Davis, "Poor Man's Air Force," 4.

[112] Davis, 5.

[113] Davis, 5.

[114] Bunker, "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs)."

[115] Davis, "Poor Man's Air Force," 6.

[116] Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence—Threats, *Suicide Bombing in the COE* (Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2005), I–3.

[117] Deputy Chief of Staff for Intelligence, II–1.

weapons that make up for in effectiveness what they lack in material sophistication."[118] When considering overall casualties and property damage, VBIEDs, both domestically and internationally, have proven to be the most effective mechanism of terrorist attack, except for the 9/11 attacks.[119] Between 2011–2016, over 21,000 deaths and injuries from VBIEDs were recorded by Action on Armed Violence and Kaaman specifically noted 73% were civilians.[120] Figure 6 illustrates the number of global suicide bombings between 2000–2015.

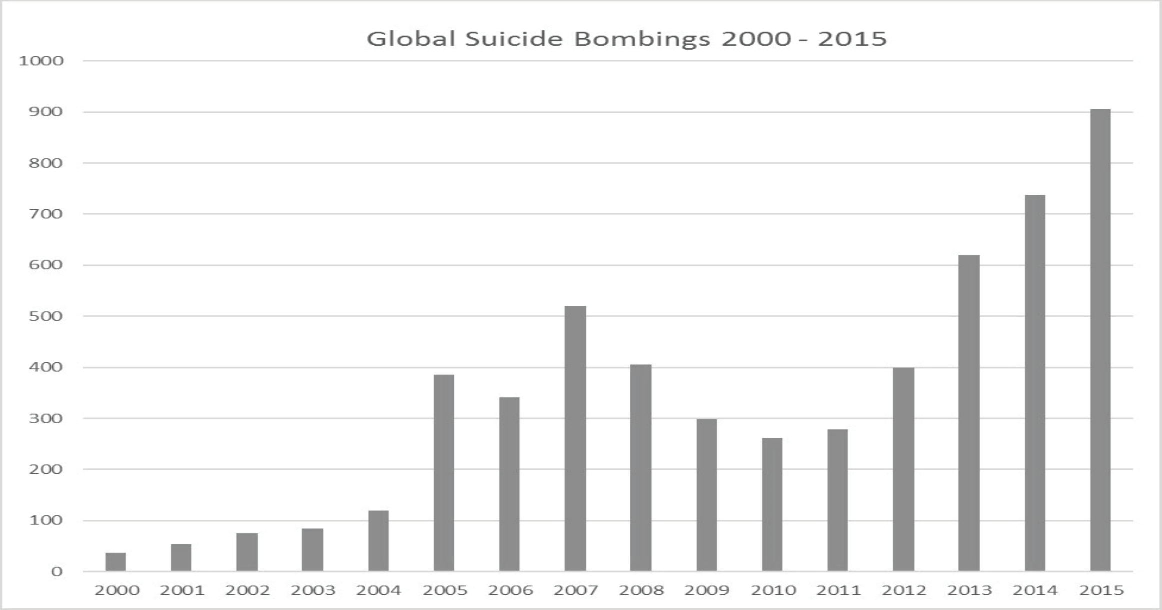


Figure 6. Global Suicide Bombings, 2000–2015[121]

Closer to home, car bombs in Mexico by cartels are primarily used as threats or warnings and terrorism within the context of psychological warfare, and secondarily, as diversionary or anti-personnel/anti-vehicular.[122] Bunker and Sullivan acknowledge

[118] Lewis, "The Human Use of Human Beings," 11.

[119] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 18.

[120] Kaaman, "The Evolution of Suicide Car Bombs Examined."

[121] Source: Lewis, "The Human Use of Human Beings," 10.

[122] Robert J. Bunker and John P. Sullivan, *Cartel Car Bombings in Mexico* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 24.

concerns about cartel car bombings associated with the drug war in Mexico spilling over into the United States.[123] With the sheer volume of suicide bombings increasing dramatically throughout the world, it does not require much imagination to predict more successful deployments in the United States.

VBIEDs pose an ongoing threat to the United States. Operational considerations by DIEDS note, “The threat of IED attack is shared almost universally by U.S. communities and citizens, private sector enterprises and public sector agencies.”[124] Between 2009 and 2015, 10 instances of intent to use VBIEDs have happened in the United States according to JCAT.[125] Currently, most of the defensive focus has been on unarmored static VBIEDs in the United States and Europe.[126] Given the success of prior attacks overseas, significant lessons can be learned.[127] Defensive strategies for the U.S. homeland need to be developed relative to the known threat of armored VBIEDs, SVBIEDs, and remote VBIEDs.[128]

VBIEDs pose a grave threat to U.S. national security. As noted by Department of Homeland Security (DHS) Secretary Michael Chertoff, “When we prioritize IEDs as a focus, we are prioritizing what is far and away the greatest threat in the West with respect to terrorist attacks.”[129] *Suicide Bombing in the COE* relates, “Unfortunately, the terrorist’s “smart bomb” doesn’t look like a bomb, and unless somehow identified is almost impossible to stop.”[130] Colonel Thomas Hammes describes the current adaptability challenge relating, “Anyone with a computer, a modem, and a credit card is

[123] Bunker and Sullivan, 34.

[124] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 32.

[125] Joint Counterterrorism Assessment Team, *VBIED-Preparedness-Recognition-Response-ONLINE-Version*, 1.

[126] Bunker, “Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs).”

[127] Joint Counterterrorism Assessment Team, *VBIED-Preparedness-Recognition-Response-ONLINE-Version*, 1.

[128] Bunker, “Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs).”

[129] Subcommittee on Domestic Improvised Explosive Devices, *Research Challenges in Combating Terrorist Use of Explosives in the United States*, 36.

[130] Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence—Threats, *Suicide Bombing in the COE*, Conclusion-1.

limited only by his own imagination and intelligence in developing information from the political level to the tactical. The last seventy years have made it clear that insurgents are imaginative, intelligent, and creative."[131] The adaptability of VBIEDs as weapons is of particular note by Kaaman, as they can function effectively in different operating environments against which they are challenging to defend.[132] Kapusta states, "Future suicide bombings within the continental United States (CONUS) are virtually guaranteed due to: the perceived success of this tactic, its proliferation across the globe and among disparate groups, and the relative ease with which such operations can be executed."[133] Collateral damage, according to Davis, is inevitable as, "If the logic of an attack is to slaughter innocents and sow panic in the widest circle, to operate a "strategy of tension," or jut demoralize a society, car bombs are ideal."[134]

3. Unmanned Aerial Vehicle Threats

UAVs were originally scarce, but as technology evolved and realized economies of scale, costs decreased and availability increased.[135] FAVs are likely to follow a similar path. This evolving technology is now so widespread that terrorists with access to UAVs have access to novel technologies suitable for asymmetrical warfare.[136] Different types of UAVs range from military specific large configurations, only available to nation states, down to small hobbyist platforms, available to the general public. Sayler addressed the classification system for discussing UAVs that Ball and Rassler embraced. Such a system helps to define the scope of this discussion to small platforms in the commercially available hobbyist category and potentially exploited by terrorists.[137] For the purpose of this discussion, UAVs can be used interchangeably with the more common nomenclature

[131] Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith Press, 2006), 195.

[132] Kaaman, "The Evolution of Suicide Car Bombs Examined."

[133] Philip E. Kapusta, "Suicide Bombers in CONUS" (monograph, School of Advanced Military Studies United States Army Command and General Staff College, 2007), 31.

[134] Davis, "Poor Man's Air Force," 7.

[135] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 11.

[136] Ball, 13.

[137] Ball, 6.

of "drone," unmanned aircraft systems (UAS), or remotely piloted vehicles (RPV). A UAV, according to the Federal Aviation Administration (FAA), is "operated without the possibility of direct human intervention from within or on the aircraft."[138] A UAS technically would also include the reference to components that control the aircraft.[139] Ball and Rassler both currently project the economic impact and sales of consumer UAVs in the United States to be in the billions of dollars, which goes to substantiate further the scope of UAV proliferation.[140]

Current regulatory challenges accompany flying UAVs in a hobbyist, commercial or government agency capacity. These challenges include operating a UAV within distinctly unique licensing or authorization criteria that many publications discuss, which shows a regulatory challenge.[141] FAA airspace requirements pose a challenge that crosses both licensing and regulatory enforcement issues.[142] Given the current lack of education and enforcement capacity, the ongoing issue with UAV operators flying in restricted airspace locations will likely lead to the implementation of additional regulations.

A regulatory option to address the restricted airspace issue could include the use of "geo-fencing" as a means to restrict airspace based on global positioning satellite (GPS) technology built into each UAV.[143] Geo-fencing offers advantages, as UAV will simply not fly in specified restricted airspace locations, such as airports and major sporting venues, thereby protecting the public and associated infrastructure. A major UAV manufacturer has preemptively incorporated geo-fencing into many of its UAV

[138] "Aeronautics and Space: Part 1—Definitions and Abbreviations," Federal Aviation Administration, Department of Transportation, *Electronic Code of Federal Regulations*, title 14 (1962), https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=a3a21673a5020d6763cfb10d068366d8&rgn=div5&view=text&node=14:1.0.1.1.1&idno=14#14:1.0.1.1.1.0.1.1.

[139] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 6.

[140] Ball, 11; Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (Lincoln Hall, West Point, NY: Combating Terrorism Center at West Point United States Military Academy, 2016), 10.

[141] Maria Valdovinos, James Specht, and Jennifer Zeunik, *Community Policing & Unmanned Aircraft Systems (UAS) Guidelines to Enhance Community Trust* (Washington, DC: Office of Community Oriented Policing Services, 2016), 50.

[142] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 17.

[143] Kevin Poulsen, "Why the U.S. Government Is Terrified of Hobbyist Drones," *WIRED*, February 5, 2015, https://www.wired.com/2015/02/white-house-drone/.

products that restricts access to over 10,000 airspace locations throughout the world.[144] Condliffe expresses concern that even geo-fencing may not stop terrorists.[145] Geo-fencing does not represent an absolute solution to protecting designated airspace since Rassler and Poulsen show how UAV technology is readily obtainable, and preventative measures are easily hacked and circumvented.[146] Discussion regarding the pros and cons of geo-fencing and how it can be defeated also apply to the deployment of FAVs, should they ever be programmed to have similar geographic travel restrictions.[147]

An overarching issue as identified by the DHS is with the recent technological advancements of UAVs and the subsequent ease of accessibility "non-state actors" have to strike against U.S. forces, allies, and law enforcement.[148] Both Rassler and Ball concur that persons with nefarious intentions already have and will continue to use repurposed (weaponized) UAVs to harm others.[149] Government sponsored studies and industry publications offer examples of when UAVs can and have been used as flying bombs for direct or indirect attacks.[150] RAND offers that UAVs are not currently an advantage based on their total destructive power, but can engage a target at a substantial distance under the control of an adversary.[151] Building upon technological advances, UAVs are increasingly becoming more autonomous, thereby decreasing their detectability as operator offset distances increase.[152]

[144] Poulsen; "DJI Introduces New Geofencing System for Its Drones," DJI Official, accessed June 26, 2018, https://www.dji.com/newsroom/news/dji-fly-safe-system.

[145] Jamie Condliffe, "Can a Chinese Drone Manufacturer's No-Fly Zone Software Stop ISIS from Weaponizing Drones?," *MIT Technology Review*, April 26, 2017, https://www.technologyreview.com/s/604279/can-djis-no-fly-zone-software-stop-isis-from-weaponizing-drones/.

[146] Rassler, *Remotely Piloted Innovation*, 17; Poulsen, "Why the U.S. Government Is Terrified of Hobbyist Drones."

[147] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 17; Rassler, *Remotely Piloted Innovation*, 49.

[148] Samantha Masunaga, "Venezuela Attack Shows Drones Can Become Assassins. Here's How They Can Be Grounded," *Los Angeles Times*, August 6, 2018, http://www.latimes.com/business/la-fi-venezuela-counterdrone-20180806-story.html.

[149] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 19; Rassler, *Remotely Piloted Innovation*, 52.

[150] Ball, 16; Marc Goodman, "How Terrorists Are Turning Robots into Weapons," Defense One, April 16, 2015, http://www.defenseone.com/ideas/2015/04/how-terrorists-are-turning-robots-weapons/110362/.

[151] Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, CA: RAND National Defense Research Institute, 2008), 26.

[152] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 21.

THIS PAGE INTENTIONALLY LEFT BLANK

II. EMERGING FAV THREATS

The intent of this section is to highlight FAV threats to help the reader have a better perspective about the overall threat environment being discussed. A need exists to encourage creativity when interacting with emerging technologies and ensuing public safety threats. Field level first responders within the homeland security enterprise will be challenged as technologies become publically available and their need to adjust to unintended consequences. Bosher and Dainty relate the need, "to examine the ways in which construction practitioners might adapt their *modus operandi* to better respond to the threats to the built environment."[153]

As a brief example, California Highway Patrol officers in the Bay Area came upon a Tesla in Autopilot mode that could be considered Level II on the vehicle automation spectrum.[154] The driver appeared to be unresponsive as the vehicle was driving down the freeway. One officer ran a traffic break to slow down traffic behind the Tesla. The other officer then positioned his patrol vehicle directly in front of the Tesla and slowed both vehicles (patrol vehicle and Tesla) to a stop. The officers then roused the Tesla driver from being asleep who was subsequently arrested for driving under the influence.[155]

A. FAV EXTERNAL THREATS—PUBLIC SAFETY

FAVs will pose a threat to homeland security due to their potential use for nefarious activities. Throughout the world, vehicles are being used as weapons, including the simple act of being driven into crowds. As recently as October 31, 2017, a terrorist drove a rented truck onto a bike path in Manhattan that killed eight people and injured a

[153] Lee Bosher and Andrew Dainty, "Disaster Risk Reduction and 'Built-in' Resilience: Towards Overarching Principles for Construction Practice," *Disasters* 35, no. 1 (2011): 5.

[154] Silver, "Autonomous Technology May Encourage a False Sense of Security."

[155] Bryan Logan, "Police Stopped a Tesla Operating on Autopilot with Drunk Driver Asleep," *Business Insider*, December 1, 2018, https://www.businessinsider.com/police-stopped-an-autopilot-driven-tesla-with-drunk-driver-asleep-2018-11.

dozen more.[156] The propensity for terrorist vehicle attacks within the United States and Europe is increasing, which is profoundly disturbing.[157] "We know these terrorists. They don't have the capability yet. But if they're trying to get people to drive a truck into crowds, then it doesn't take too much imagination to think they are going to take an autonomous car and drive it into a crowd of people," said John Carlin, assistant U.S. attorney general for national security.[158] The FBI predicts FAVs, "will have a high impact on transforming what both law enforcement and its adversaries can operationally do with a car."[159]

Adding to the challenge of FAV use moving forward, traditionally, criminals are quick to adapt to new technology and law enforcement is not. The FBI has already predicted FAV scenario where, "bad actors will be able to conduct tasks that require use of both hands or taking one's eyes off the road which would be impossible today." An added caveat is that suspects could be shooting at pursuers while the getaway car is driving itself.[160] Another report generated within the FBI's Directorate of Intelligence relates, "Autonomy … will make mobility more efficient, but will also open up greater possibilities for dual-use applications and ways for a car to be more of a potential lethal weapon than it is today."[161] This report then goes on to provide different examples of FAV misuses by those who may cause this nation harm, which is further discussed in this thesis.[162]

[156] Shimon Prokupecz et al., "ISIS Note Found near Truck Used in Manhattan Terror Attack," CNN, November 6, 2017, http://www.cnn.com/2017/10/31/us/new-york-shots-fired/index.html.

[157] Jake Gibson, "Timeline of Recent Vehicle Attacks in U.S., Europe," Fox News, November 1, 2017, http://www.foxnews.com/world/2017/11/01/timeline-recent-vehicle-attacks-in-us-europe.html.

[158] Jeffrey Massimilia, "Connected, Self-Driving Cars Pose Serious New Security Challenges," IndustryWeek, July 25, 2016, http://www.industryweek.com/emerging-technologies/connected-self-driving-cars-pose-serious-new-security-challenges.

[159] Harris, "FBI Warns Driverless Cars Could Be Used as 'Lethal Weapons.'"

[160] Harris.

[161] Harris.

[162] Harris.

B. THREAT OF FAV ARMED WITH VBIED

The availability of FAVs will change terrorism tactics, as the need for VBIED martyrdom operations will decrease as acquisition of FAVs becomes easier. Terrorists throughout the world currently use VBIEDs. They have become commonplace in the Middle East, as they are frequently used by terrorist organizations. One of the first crude VBIEDs is credited to anarchist Mario Buda.[163] During September 1920 in Manhattan, he blew up a horse and wagon that caused numerous fatalities and injuries.[164] VBIEDs have since evolved significantly.

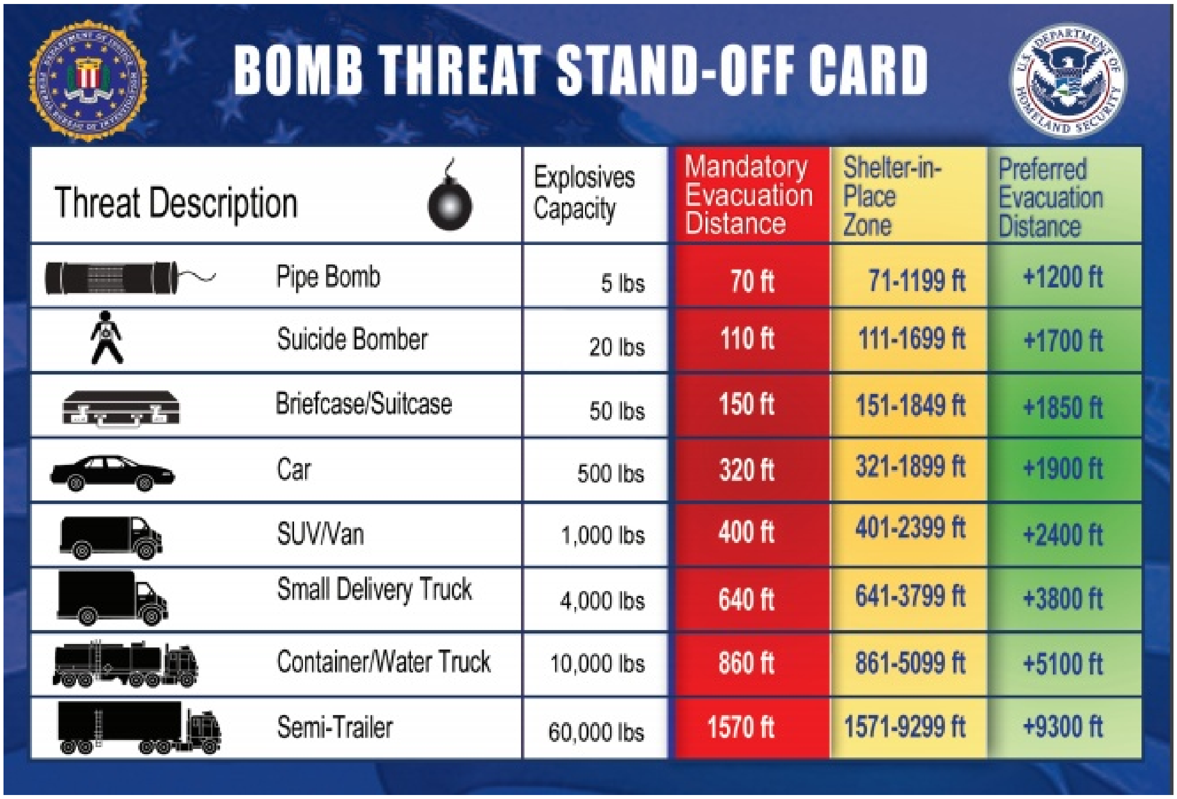
Contemporary vehicular suicide attacks can be traced to April 1983 when Hezbollah attacked western targets in Lebanon. In one particular instance, a suicide bomber attacked the U.S. Embassy with a VBIED and killed 63 people.[165] Other VBIED attacks on the U.S. mainland have since occurred. Most notably were the VBIED attacks of the World Trade Center in 1993 and the Murrah Federal Building in 1995. Both attacks used large rented vehicles.[166] Figure 7 from the DHS provides the *Bomb Threat Stand-Off Card* for different explosive configurations including vehicles.

[163] Davis, “Poor Man’s Air Force,” 4.

[164] Davis, 4.

[165] Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence—Threats, *Suicide Bombing in the COE*, I–3.

[166] Department of Homeland Security, *Potential Threat to Homeland Using Heavy Transport Vehicles* (Washington, DC: Department of Homeland Security, 2004), 3.



BOMB THREAT STAND-OFF CARD

Threat Description	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
Pipe Bomb	5 lbs	70 ft	71-1199 ft	+1200 ft
Suicide Bomber	20 lbs	110 ft	111-1699 ft	+1700 ft
Briefcase/Suitcase	50 lbs	150 ft	151-1849 ft	+1850 ft
Car	500 lbs	320 ft	321-1899 ft	+1900 ft
SUV/Van	1,000 lbs	400 ft	401-2399 ft	+2400 ft
Small Delivery Truck	4,000 lbs	640 ft	641-3799 ft	+3800 ft
Container/Water Truck	10,000 lbs	860 ft	861-5099 ft	+5100 ft
Semi-Trailer	60,000 lbs	1570 ft	1571-9299 ft	+9300 ft

Figure 7. Bomb Threat Stand-Off Card[167]

A Type 1 VBIED, as discussed by Bunker, shows several characteristics typified as a vehicle readily available to the public (as opposed to a military vehicle), parked (or static), unarmored, with the driver often leaving the area prior to it exploding.[168] Type 2 VBIEDs are simply a Type 1 VBIED driven into the intended target prior to being exploded by a martyr.[169] The most recent evolution of VBIEDs is the Type 3, which is an up armored Type 2 that can further penetrate defenses prior to exploding.[170]

When a FAV is equipped with an explosive device, it turns into a Type 2 VBIED, without a driver! Depending on the target, a human presence may still be needed.

[167] Source: TRIPwire, *DHS-DOJ Bomb Threat Stand-off Card* (Washington, DC: Department of Homeland Security, n.d.), accessed January 21, 2019, https://tripwire.dhs.gov/IED/resources/docs/DHS-DOJ%20Bomb%20Threat%20Stand-off%20Card.pdf.

[168] Bunker, "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs)."

[169] Bunker.

[170] Bunker.

However, FAVs could potentially be equipped with armor and operate in a Type 3 VBIED capacity. To address VBIED concerns, James Niles, president of Orbit City Labs, urged the government to require sensors capable of detecting hazardous materials in autonomous vehicles at an NTSB hearing. Niles stated, “You could have the safest vehicle, the highest cybersecurity, and the tightest control of privacy data and still be wide open for bad actors to load the vehicle up with explosives, punch in coordinates, shut the door and send the vehicle to its destination.”[171]

Now consider the use of a big rig as a VBIED. The scale of devastation would increase substantially. A fully loaded tractor-trailer semi would dwarf the explosion that occurred in Oklahoma, as earlier referenced. Even more disturbing is the fact that overseas shipping containers are often sealed and delivered from their respective ports to different locations without the driver even knowing what is being shipped, except for a generalized bill of lading. It does not take much of an imagination to think of the destructive capabilities that could be garnered from this nation’s soon to be fully automated ports and related fully autonomous commercial shipping. As an aside, these fully autonomous ports would be staffed by the remaining angry longshoremen and commercial drivers who managed to retain employment at a lower pay rate as their former jobs were displaced by this new technology.[172]

C. FAV INTERNAL THREATS—OCCUPANT SAFETY

Hacking autonomous vehicles is a threat to homeland security. Experts from vastly different backgrounds have expressed consternation regarding the future threat of hacking FAVs. General Motors Chief Executive Officer Mary Barra commented that car security will be a significant public safety issue and stated, “A cyber incident is not a

[171] Baker, “How Self-Driving Cars Could Become Weapons of Terror.”

[172] Rachel Uranga, “Port of L.A.’s Automated Terminal: Future of Commerce or Blue-Collar Job-Killer?,” *Press Telegram* (blog), March 18, 2017, http://www.presstelegram.com/business/20170318/port-of-las-automated-terminal-future-of-commerce-or-blue-collar-job-killer.

problem just for the automaker involved. It is a problem for every automaker around the world."[173]

Current day non-autonomous vehicles are already susceptible to hacking. Vehicle hacking according to Rouse is, "the manipulation of the code in a car's electronic control unit (ECU) to exploit a vulnerability and gain control of other ECU units in the vehicle."[174] Greenberg references a Department of Transportation Public Safety Advisory when stating:

> Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience… Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cybersecurity threats.[175]

Connectivity impacts everyone as the vehicles may be susceptible to hacking. Even if this vulnerability does not apply to an individual's vehicle, simply using roads and freeways means people are likely interacting with susceptible vehicles.

Current vehicles are increasingly becoming more vulnerable to widespread cyber-attacks as a result of being connected to different technological systems including the "Internet of things (IoT)."[176] Modern cars contain dozens of ECUs connected by means of an internal network. These vehicles then have the potential to be susceptible as hackers look to gain access through a vulnerable ECU and navigate the system to take control of vital vehicle components, such as the engine or brakes.[177] ECUs can wirelessly access

[173] Will Knight, "GM's CEO, Mary Barra, Says the Threat of Cars Being Hacked Will Pose a Risk to the Entire Car Industry," *MIT Technology Review*, July 22, 2016, https://www.technologyreview.com/s/601957/gm-ceo-car-hacking-will-become-a-public-safety-issue/.

[174] "What Is Car Hacking?," IoT Agenda, November 5, 2017, http://internetofthingsagenda.techtarget.com/definition/car-hacking.

[175] Andy Greenberg, "The FBI Warns That Car Hacking Is a Real Risk," WIRED, March 17, 2016, https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/.

[176] Bridget Clerkin, "How Will We Ensure Security in a Self-Driving World?," DMV, September 21, 2017, https://www.dmv.org/articles/cybersecurity-and-self-driving-cars.

[177] Murray Slovick, "Security Issues Could Still Crimp the Self-Driving Car," Electronic Design, June 28, 2017, http://www.electronicdesign.com/automotive/security-issues-could-still-crimp-self-driving-car.

critical driving functions through unsecure internet-enabled gadgets plugged into connection points people often utilize for simple tasks, such as diagnostics or an insurance company driver's discount monitoring devices.[178] Additionally, external connectivity access points include remote vulnerabilities from different networks manufacturers may have built into the vehicles to push out system updates wirelessly, as currently done by Tesla.[179] An FBI public service announcement states, "Vulnerabilities may exist within a vehicle's wireless communication functions, within a mobile device—such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi—or within a third-party device connected through a vehicle diagnostic port."[180]

Hacking vehicles' various ECUs requires identifying a series of vulnerabilities. Greenberg provided an example when researchers, "could burrow through the Wifi connection of a Tesla S all the way to its driving systems and remotely activate the moving vehicle's brakes, they exposed a chain of security problems."[181] Other examples of hacking, such as with a Jeep Cherokee, have shown it is possible to access a vehicle's infotainment system and then subsequently access its steering and brakes.[182] Another demonstration included a Corvette that had its brakes remotely activated and deactivated via cell phone control.[183] Many other hacking examples also include using the internet to access critical ECU systems for vehicles from additional major manufacturers.[184] Vulnerabilities are not a guarantee of worst-case ECU hacking scenarios, but any possible nefarious system access is a public safety concern.[185]

[178] Andy Greenberg, "Hackers Cut a Corvette's Brakes via a Common Car Gadget," WIRED, August 11, 2015, https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/.

[179] Andy Greenberg, "Tesla Responds to Chinese Hack with a Major Security Upgrade," WIRED, September 27, 2016, https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/.

[180] "Motor Vehicles Increasingly Vulnerable to Remote Exploits," Federal Bureau of Investigation, March 17, 2016, https://www.ic3.gov/media/2016/160317.aspx; Andy Greenberg, "A New Wireless Hack Can Unlock 100 Million Volkswagens," WIRED, July 10, 2016, https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/.

[181] Greenberg, "Tesla Responds to Chinese Hack with a Major Security Upgrade."

[182] Greenberg, "Hackers Cut a Corvette's Brakes via a Common Car Gadget."

[183] Greenberg.

[184] Greenberg, "Securing Driverless Cars from Hackers Is Hard."

[185] Federal Bureau of Investigation, "Motor Vehicles Increasingly Vulnerable to Remote Exploits."

Auto manufacturers are frequently very slow to fix problems they have uncovered due, in part, to the slow software development cycle. As such, resolving issues is not a speedy process.[186] Of specific concern is the fact new vehicles still frequently utilize 1990s security techniques, which will not be acceptable with the advent of fully autonomous interconnected vehicles.[187] Unless better regulatory language is developed to address these concerns, ECUs will likely remain susceptible as “best practices,” “guidance,” and “should” lack imperative that translates into vulnerability.[188]

Consider the ability to deactivate a single moving vehicle’s breaking system remotely that can harm the driver and whatever else the vehicle hits. Imagine now not just one vehicle having its brakes remotely deactivated or activated (such as a Jeep Cherokee or Corvette), but hundreds, thousands, or hundreds of thousands. Stefan Gudmundson stated, “We’re lucky that no one has hacked an entire brand of cars and said, I’m going to stop all your cars tomorrow at noon, unless you give me money.”[189] A person can deactivate an engine or disable the brakes and demand untraceable bitcoins to restore the vehicle to an operational state and criminals prefer low risk exploits with minimal effort and maximum reward.[190] Welcome to the world of Ransomware.[191]

NHTSA Administrator Dr. Mark Rosekind commented on current vehicle system vulnerabilities and stated, “Everyone involved must keep moving, adapting, and improving to stay ahead of the bad guys.”[192] Cybersecurity will continue to rise in

[186] Greenberg, “A New Wireless Hack Can Unlock 100 Million Volkswagens.”

[187] Greenberg.

[188] Carl Herberger, “Why the Department of Transportation’s Self-Driving Car Guidelines Aren’t Enough,” *TechCrunch* (blog), November 6, 2016, http://social.techcrunch.com/2016/11/06/why-the-department-of-transportations-self-driving-car-guidelines-arent-enough/.

[189] Pete Bigelow, “Auto Industry Unites to Take Countermeasures against Hackers,” Car and Driver, June 10, 2016, https://blog.caranddriver.com/auto-industry-unites-to-take-countermeasures-against-hackers/.

[190] Chris Poulin, “Connected Car Security: Separating Fear from Fact,” *TechCrunch* (blog), October 23, 2015, http://social.techcrunch.com/2015/10/23/connected-car-security-separating-fear-from-fact/.

[191] “Ransomware,” US-CERT United States Computer Emergency Readiness Team, accessed January 22, 2019, https://www.us-cert.gov/Ransomware.

[192] “Guidance Covers Cybersecurity Best Practices for All Motor Vehicles, Individuals and Organizations Manufacturing and Designing Vehicle Systems and Software,” National Highway Transportation Safety Agency, October 24, 2016, https://www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle.

importance as self-driving cars become available to the general public and private industry. Simply put, as Herberger states, "If your computer gets hacked it can be costly… If your car gets hacked it can be deadly."[193] Currently, some of the easiest ransomware targets tend to be critical establishments, such as medical facilities and law enforcement agencies, because more is at stake when these institutions become victims.[194] How will ransomware be perceived relative to FAVs when they are finally made available on a large scale to the general public? "Autonomous vehicles are at the apex of all the terrible things that can go wrong. Cars are already insecure, and you're adding a bunch of sensors and computers that are controlling them... If a bad guy gets control of that, it's going to be even worse," as stated by Charlie Miller, former member of the National Security Agency's (NSA) Tailored Access Operations team of elite hackers.[195] RAND Senior Information Scientist Nidhi Kalra also related with regard to the hacking of autonomous vehicles:

> It is a very real threat… it's a way to disrupt our transportation system. So there's a great concern there… And it's not only hacking for fun and profit, but autonomous vehicles provide an avenue for terrorism as well because there's a way to use these vehicles to… blow themselves up… we need to think very broadly about cybersecurity, not only as a hacking opportunity but also as a terrorism opportunity.[196]

D. PARALLEL TECHNOLOGY THREATS—UAV THREATS ASSESSMENT

What can be learned from parallel technology threats? As FAVBIEDs have yet to be deployed throughout the world, it is necessary to look toward other technologies that may have similar concerns regarding their accessibility to the public and adoptability for dual-use nefarious purposes. One such example is UAVs, specifically sUAVs. sUAVs are

[193] Herberger, "Why the Department of Transportation's Self-Driving Car Guidelines Aren't Enough."

[194] Annie Sneed, "The Most Vulnerable Ransomware Targets Are the Institutions We Rely on Most," *Scientific American*, March 23, 2016, https://www.scientificamerican.com/article/the-most-vulnerable-ransomware-targets-are-the-institutions-we-rely-on-most/.

[195] Greenberg, "Securing Driverless Cars from Hackers Is Hard."

[196] Susan Jones, "'Autonomous Vehicles Provide an Avenue for Terrorism,' Congress Is Told," CNSNews, February 15, 2017, https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told.

becoming increasingly available as technological and manufacturing improvements make these products accessible to a larger audience. With the rapid advancement of this new technology, it is evident the regulatory environment has failed to keep pace and provide the law enforcement and regulatory community with resources needed to ensure public safety. Although sUAVs have capabilities that can benefit society, they also can be repurposed for those with despicable intentions. As Ball relates, "With the private sector serving as the primary catalyst of innovation and technology advancement, this increasingly available dual-use technology is well-suited for asymmetrical warfare."[197]

Emerging counter-drone technologies can disable sUAVs in-flight, such as jamming or controlling radio frequencies, nets, directed-energy systems, and compact laser weapons.[198] Other regulatory options include the previously discussed use of "geo-fencing."[199] Even unintentionally, hobbyist sUAV operations have revealed security and public safety weaknesses throughout the world. Examples include a sUAV operator who has been convicted of multiple offenses in Great Britain for flying over restricted areas including the Houses of Parliament, Buckingham Palace, and different football stadiums (aka soccer in the United States).[200] Within the United States, multiple incidents have occurred where drones have been illegally operated within FAA designated "no-drone zones." One operator unsuccessfully attempted to photograph the Washington Monument when he crashed his sUAV onto White House grounds.[201] Chancellor Angela Merkel also had a drone crash near her at a campaign event.[202] Even within California, first

[197] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 13.

[198] Masunaga, "Venezuela Attack Shows Drones Can Become Assassins."

[199] Poulsen, "Why the U.S. Government Is Terrified of Hobbyist Drones."

[200] James Chapple and Agency staff, "Man Fined for Flying Drone over Parliament and Buck Palace," MyLondon, September 16, 2015, http://www.getwestlondon.co.uk/news/west-london-news/man-fined-flying-drone-over-10063456.

[201] Bart Jensen, "Small Drone Crashes near White House despite Ban against Flights in D.C.," USA TODAY, October 9, 2015, https://www.usatoday.com/story/news/2015/10/09/drone-crash-white-house-ellipse-us-park-police-federal-aviation-administration/73641812/.

[202] Masunaga, "Venezuela Attack Shows Drones Can Become Assassins."

responders have had significant impacts to their operations as a result of irresponsible sUAV pilots, and in another example, caused firefighting aircraft to be grounded.[203]

President Nicolas Maduro recently survived a "drone assassination attempt" when he was attending a ceremony recognizing the 81st anniversary of the Venezuelan army.[204] The Venezuelan Interior, Justice and Peace Minister, Nestor Reverol, related that each of the two DJI M600 drones carried approximately one kilogram of C-4 explosive.[205] One drone lost control and crashed prior to reaching presentation area while the second drone exploded and injured seven guardsmen.[206]

Terrorist interest in using drones is not a new phenomenon. Approximately two decades ago, one of the first documented terror cases occurred when a fanatical group, Aum Shinrikyo, plotted to deploy sarin gas via drone in Japan.[207] Although current sUAV uses by terrorist groups lean toward surveillance and communications, instances have resulted in which they have been weaponized, but not to the extent that the outcome of a battle was altered.[208] As with other technological advancements, necessity is the mother of invention and it is only a matter of time before off the shelf sUAVs will be adapted with increasing frequency for despicable purposes.

When discussing the topic of UAVs, a basic understanding of the different taxonomy needs to be addressed as UAVs vary in size, weight, range, accessibility, payload capacity, and affordability. Ball's graphic in Figure 8 describes the differences

[203] Patrick May, "Firefighters Decry Drone Interference—One Pilot Arrested," *Mercury News*, October 16, 2017, https://www.mercurynews.com/2017/10/16/firefighters-say-drones-interfered-with-their-work-one-pilot-arrested/.

[204] "Venezuela President Maduro Survives 'Drone Assassination Attempt,'" *BBC News*, sec. Latin America & Caribbean, August 5, 2018, https://www.bbc.com/news/world-latin-america-45073385.

[205] Chris Kraul and Mery Mogollon, "Venezuela Says Assassination Attempt Used Drones Loaded with 2 Pounds of Plastic Explosives," *Los Angeles Times*, August 5, 2018, http://www.latimes.com/world/la-fg-venezuela-drone-attack-20180805-story.html.

[206] Kraul and Mogollon.

[207] Rassler, *Remotely Piloted Innovation*, 13.

[208] Rassler, 44.

and this discussion focuses on sUAVs, as they are the most widely available and most frequently used by both hobbyist and terrorist groups.[209]

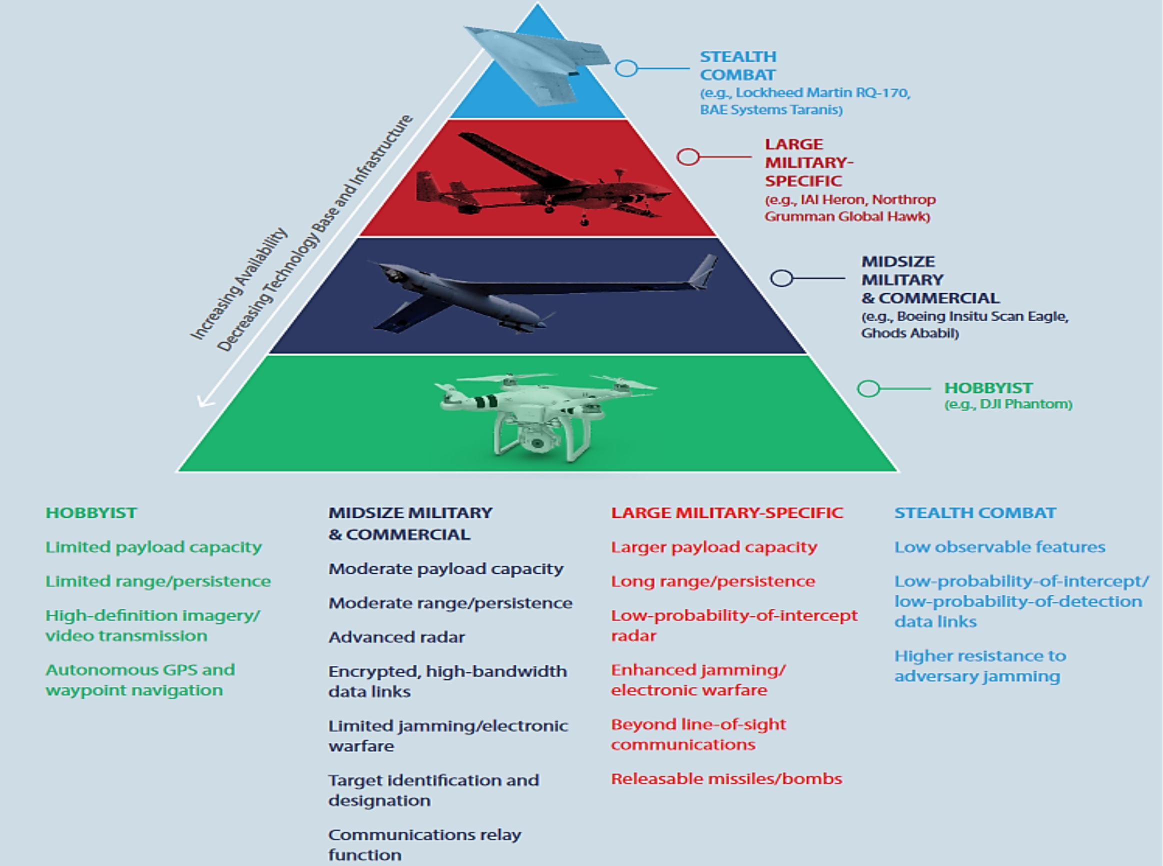

STEALTH COMBAT
(e.g., Lockheed Martin RQ-170, BAE Systems Taranis)
LARGE MILITARY-SPECIFIC
(e.g., IAI Heron, Northrop Grumman Global Hawk)
MIDSIZE MILITARY & COMMERCIAL
(e.g., Boeing Insitu Scan Eagle, Ghods Ababil)
HOBBYIST
(e.g., DJI Phantom)
Increasing Availability
Decreasing Technology Base and Infrastructure
HOBBYIST
Limited payload capacity
Limited range/persistence
High-definition imagery/ video transmission
Autonomous GPS and waypoint navigation
MIDSIZE MILITARY & COMMERCIAL
Moderate payload capacity
Moderate range/persistence
Advanced radar
Encrypted, high-bandwidth data links
Limited jamming/electronic warfare
Target identification and designation
Communications relay function
LARGE MILITARY-SPECIFIC
Larger payload capacity
Long range/persistence
Low-probability-of-intercept radar
Enhanced jamming/ electronic warfare
Beyond line-of-sight communications
Releasable missiles/bombs
STEALTH COMBAT
Low observable features
Low-probability-of-intercept/ low-probability-of-detection data links
Higher resistance to adversary jamming

Figure 8. Taxonomy of UAVs[210]

With over three million in global sales for sUAVs, and commercial UAVs in 2016 and global revenue of over $4 billion, it will continue to be difficult to prevent terrorists from acquiring this technology.[211]

One of the challenges with sUAVs is the identification of the owner/pilot. With user offset distances that could be several miles, no current mechanism exists to remotely

[209] Ball, *The Proliferation of Unmanned Aerial Vehicles*, 11.

[210] Source: Ball, 6.

[211] Ball, 11.

identify a person flying the sUAV. Owners are required to have their identifying information on the sUAV; however, given the size, it is unrealistic to think this information could be visually observed, as the aircraft could be flying at an altitude of several hundred feet. The FAA is considering mandating a remote identification capability for sUAVs. However, it is unlikely it will be implemented in the foreseeable future, as national mandates frequently have to travel challenging paths for success.

Given sUAVs are present throughout the world, it is reasonable and prudent to consider how other nations or regions are addressing their similar regulatory and public safety challenges. Both Denmark and Italy have codified regulations regarding sUAV remote identification, albeit currently unenforceable.[212] Several other countries have proposed sUAV remote identification requirements along with the European Union. Germany understands the concept of sUAV remote identification but chooses not to engage with the issue to avoid projected regulatory costs.[213] Given the acknowledgement of this worldwide concern, manufacturers of sUAVs are also preemptively considering enacting solutions for remote identification and other concerns agreeable to both law enforcement and different stakeholder communities.[214]

[212] Da-Jiang Innovations, *DJI Remote Identification Whitepaper* (Nanshan District, Shenzhen, China: Da-Jiang Innovations, 2017), 1, https://www.dropbox.com/s/v4lkyr2kdp8ukvx/DJI%20Remote%20Identification%20Whitepaper%203-22-17.pdf?dl=0.

[213] CEPT Electronic Communications Committee, *Technical and Regulatory Aspects and the Needs for Spectrum Regulation for Unmanned Aircraft Systems (UAS)*, ECC Report 268 (Copenhagen, Denmark: CEPT Electronic Communications Committee, 2017), 23, https://www.cept.org/files/9522/Draft%20ECC%20Report%20268%20for%20PC.docx.

[214] Gary Mortimer, "UAvionix Release Remote Identification White Paper," *SUAS News—The Business of Drones* (blog), 2, April 4, 2017, https://www.suasnews.com/2017/04/uavionix-release-remote-identification-white-paper/.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FAVBIED MITIGATING STRATEGIES

Why a mitigating strategy? The purpose of a strategy is to have a high-level view of the topic being addressed relative to its operational environment. Having a strategy will establish a framework about how public safety decisions and priorities will be made.[215] This discussion intends to provide concepts, some general, some specific, whereby the threat of FAVBIEDs can be avoided or at least minimized. To think that the threat of terrorism could be eliminated is entirely unreasonable. As with terrorism, the threat presented by the nefarious use of FAVs will always be present. As with infrastructure protection, the goal is not to make something so hardened it is inaccessible and thereby unusable, it is merely to make a target sufficiently uninviting. In this instance, making FAVs less appealing as a mechanism of terror is the preferred outcome.

A. RESEARCH DESIGN

Research Question: What fully autonomous vehicle technologies could be adapted to mitigate the threat of VBIEDs?

This research on strategies to mitigate the threat of FAVs being used as VBIEDs incorporates several different components. This effort seeks to document the emerging threat posed by FAVs. The FAV threat has an internal component addressing the safety of vehicle occupants and an external component addressing the safety of the general public. An existing body of literature addresses the use of VBIEDs throughout the world and specific examples of deployments within the United States. Parallels can be drawn from recent technological advancements, such as the increasing availability of sUAVs, including their usage by terrorists and governmental regulatory gaps.

1. FAVBIED Mitigating Strategy Loop

The thesis also uses a framework of developing mitigating-dual-use technology adaptations by considering different fully autonomous VBIED (FAVBIED) scenarios.

[215] Ann Latham, “What The Heck Is A Strategy Anyway?,” *Forbes*, October 29, 2017, https://www.forbes.com/sites/annlatham/2017/10/29/what-the-heck-is-a-strategy-anyway/.

The scenarios selected are created from predicted FAV uses complemented by prior terrorism incidents. Discussion comingles the use of current and projected FAV technologies. The proposed mitigating strategies are developed in an actionable sequence of *before*, *during*, and *after* an event. In some instances, autonomous vehicle technologies have applications which, when combined, will propose an elegant solution. This elegant solution is inspired by the law of parsimony with a quote attributed to Einstein when he stated, "Everything should be made as simple as possible, but not simpler."[216] Since the threat of terrorism to the U.S. homeland can be considered an uncontrollable external low occurrence risk, the intent of this thesis is not only to identify risks, but also acknowledge the potential impact and determine how to mitigate the effects if indeed an event does occur.[217] Therefore, selecting a concise, yet diverse, set of scenarios will communicate innovative ideas and stimulate further discussion, research, and implementation while avoiding complexity bias.[218]

Figure 9 depicts a FAVBIED mitigating strategy loop. Mitigating strategies can be applied *before* an event to deter it from happening, *during* an event to minimize the impact, and *after* an event to allow for follow-up and lessons learned. Then the lessons learned are subsequently applied to successive *before, during,* and *after* mitigating strategies, and the cycle will repeat itself. Additionally, as learning and technological evolution occurs, adaptation to any portion of this mitigating strategy loop can be applied outside of an event as well.

[216] Phil Gibbs and Sugihara Hiroshi, "What Is Occam's Razor?," University of California, Riverside, Department of Mathematics, 1997, http://math.ucr.edu/home/baez/physics/General/occam.html.

[217] Kaplan and Mikes, "Managing Risks."

[218] "Complexity Bias: Why We Prefer Complicated to Simple," *Farnam Street* (blog), January 8, 2018, https://fs.blog/2018/01/complexity-bias/.

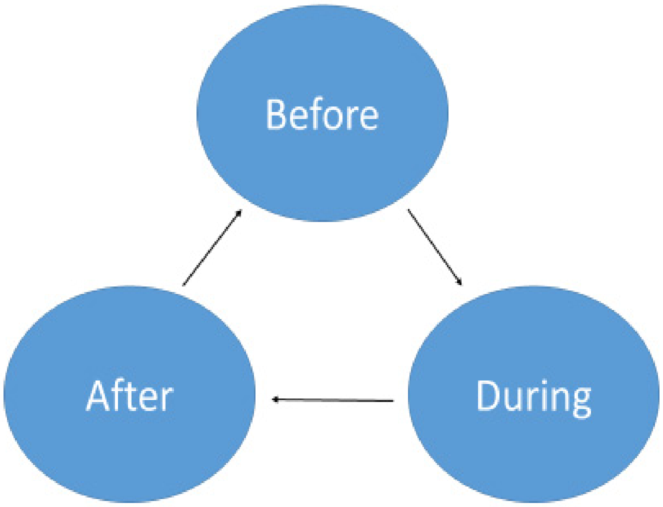


Figure 9. Fully autonomous vehicle-borne improvised Explosive Device Mitigating Strategy Loop

2. Scope

Related topics involving political, ethical, privacy and legal aspects to the deployment of FAVs lie beyond the scope of this thesis. The intent is to present mitigating strategies private industry can embrace on its own accord, as the current prevailing governmental strategy promotes a "hands off" approach in an effort to avoid inhibiting technological development in this rapidly evolving and highly competitive industry.[219] As such, this thesis looks to avoid specific governmental policy recommendations or mandates. Additionally, this exploration only incorporates the utilization of fully autonomous passenger vehicles as opposed to commercial vehicles.

3. Risk Assessment

The General Guidelines on Risk Assessment by the National Research Council states:

[219] Aaron Saltzman, "As Risky as It Sounds, a Hands-off Approach to Driverless Vehicle Safety May Save Lives," CBC News, September 15, 2017, http://www.cbc.ca/news/business/autonomous-vehicles-self-driving-cars-uber-google-general-motors-1.4287591.

> Risk may be defined as a measure of the probability of an unwanted event and the impact of that event. Risk assessment is a synthesis and summary of information about a potentially hazardous situation that addresses the needs and interests of decision-makers and of interested and affected parties.[220]

To prioritize and assess risk, analysis should consider both the probability and consequences of a particular risk event. As this thesis explores the use of a technology that has yet to be commercially available to the general public, the probability of a FAVBIED is currently considered low. However, as Mathis states, "Most individuals and organizations have not yet realized that low-probability risks are really a major factor in their safety experiences."[221] The consequences of a future successful deployment would be considerable. For an example of what was perceived as a low probability event with a considerable outcome, look no further to when on 9/11 air traffic controllers grounded all flights within the United States after the air strikes and the ensuing sizable impact to both lives lost and the U.S. economy.[222] Would it be surprising to see a similar occurrence for all FAVs when eventually used in a successful terrorist deployment as a FAVBIED?

When considering risk assessment, it is very important to identify external risks (which are largely uncontrollable), gauge their likely impact, and identify how to minimize their effects should they occur.[223] Grabowski et al. discuss:

> The process of performing a risk assessment includes the identification of the series of events leading to an accident, estimation of the probabilities of identification of the series of events leading to an accident, estimation of the probabilities of these events and the evaluation of the consequences of different degrees of system failure.[224]

[220] Martha Grabowski et al., *The Washington State Ferries Risk Assessment Final Report* (Washington, DC: The George Washington University; Troy, NY: Rensselaer Polytechnic Institute; Richmond, VA: Virginia Commonwealth University, 1999), 15.

[221] Terry Mathis, "Low Probability Risks Can't Be Ignored," The Compass, ASSE Management Practice Specialty Newsletter, June 2003.

[222] Thomas H. Kean and Lee Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: National Commission on Terrorist Attacks, 2004), 29.

[223] Kaplan and Mikes, "Managing Risks."

[224] Grabowski et al., *The Washington State Ferries Risk Assessment Final Report*, 17.

It is difficult to predict low-probability events, and consequently, they are challenging to define, recognize, and prevent.[225] Risk management looks to offer actions and suggest policies or strategies for threat reduction posed by vulnerabilities.[226] The intent is for risk management to consider cost effective risk strategies that will have a wide ranging impact over the totality of the topic being engaged, in this case FAVBIEDs or even just FAVs.[227] As Mathis relates, "These strategies often involved preventive measures that must be taken hundreds or thousands of times with no apparent result to be effective."[228] The FAV utilization sample size or global market, albeit currently considered nonexistent, is projected to increase profoundly once it becomes available to the general public.[229] Lastly, the best ideas come from within and a collaborative effort by the involved stakeholders will have a higher likelihood of implementation.

The risk management process (Figure 10) used in this analysis identifies external and internal factors that will impact the ability to mitigate the threat of FAVs being used as bombs.[230] Risk is identified and assessed, and control measures are determined in an effort to prioritize decisions.[231] When looking at the implementation of risk controls or monitor and review, consideration is given to what may potentially be measured for a return on investment (ROI) discussion as related to future steps.[232] The final output prioritizes strategies in a framework easily relatable to transportation industry technological expectations and translates the imperative for stakeholders to adopt strategies preemptively to counter a predictable national security threat.

[225] Mathis, "Low Probability Risks Can't Be Ignored."

[226] Grabowski et al., *The Washington State Ferries Risk Assessment Final Report*, 17.

[227] Grabowski et al., 17.

[228] Mathis, "Low Probability Risks Can't Be Ignored."

[229] Garsten, "Sharp Growth in Autonomous Car Market Value."

[230] ECRRN European Cyber Resilience Research Network, "6 Steps Risk Management Approach."

[231] ECRRN European Cyber Resilience Research Network.

[232] ECRRN European Cyber Resilience Research Network.

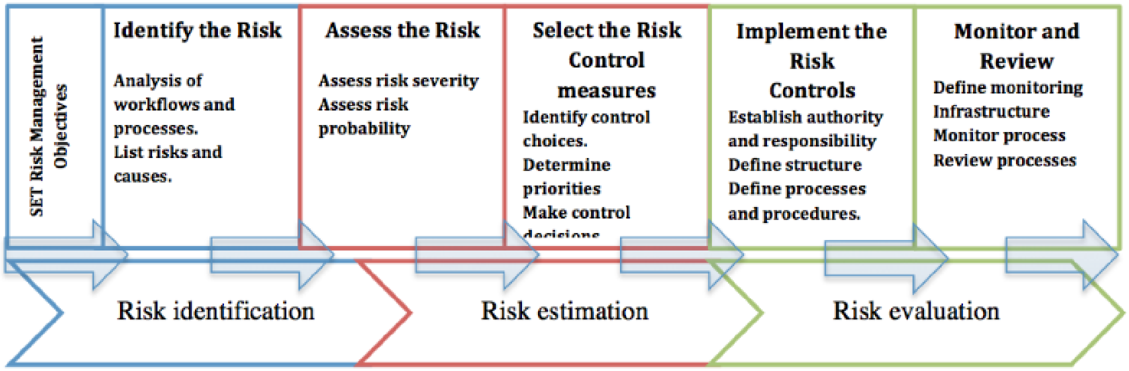


Figure 10. Risk Management Process[233]

B. THOUGHT EXPERIMENTS

Why present threats and identify mitigating strategies using scenarios? By using thought experiments, it is then possible to examine what can be known, learned from mistakes and how to avoid future mistakes.[234] Ernst Mach writes:

> Our own ideas are more easily and readily at our disposal than physical facts. We experiment with thought, so as to say, at little expense. This it shouldn't surprise us that, often time, the thought experiment precedes the physical experiment and prepares the way for it.[235]

Using scenarios makes it possible to visualize potential future threats based, in part, on extrapolating from past events and blending them into current and projected reality. This nation is now in a unique position to anticipate threats that will have deadly consequences in the immediate future.

C. TERRORIST ATTACK PLANNING CYCLE

In anticipating the use of FAVBIEDs by terrorists, a lens to visualize the process by which they make their plans needs to be available. An exact defined system is not in

[233] Source: ECRRN European Cyber Resilience Research Network.

[234] "Mental Models: The Best Way to Make Intelligent Decisions (109 Models Explained)," *Farnam Street* (blog), accessed January 13, 2019, https://fs.blog/mental-models/.

[235] Ernst Mach, *On Thought Experiments*, trans. W. O. Price and Sheldon Krimsky (Medford, MA: Tufts University, 1972), 452, https://sites.tufts.edu/sheldonkrimsky/files/2018/05/pub1973OnThought Experiments.pdf.

place that all terrorists use to achieve their objectives. However, many of the visual representations developed commonly have the following phases represented as in Figure 11.

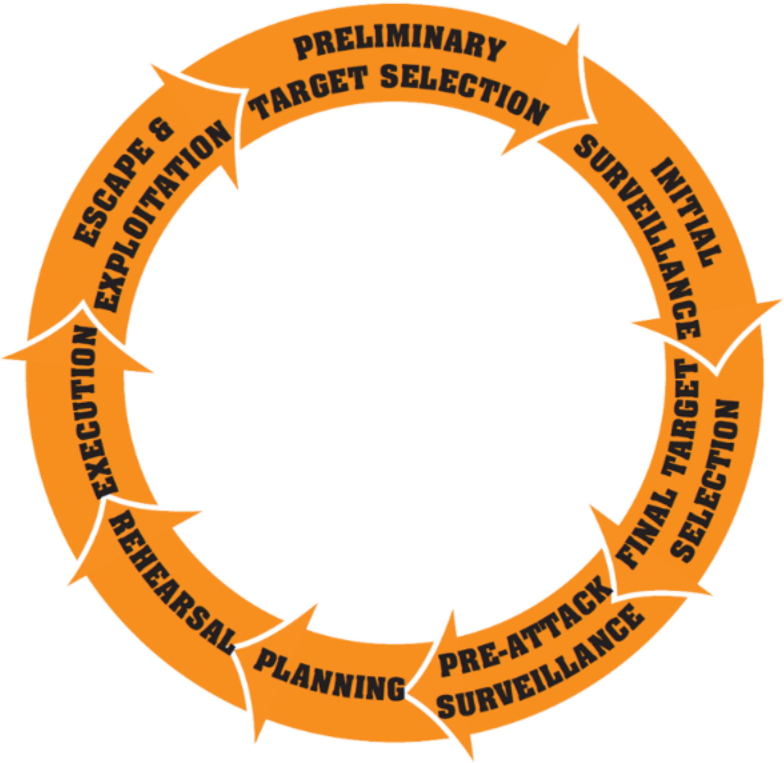


Figure 11. Terrorist Planning Cycle[236]

As opposed to martyrdom operations (aka suicide bombers), the use of a FAVBIED presents unique challenges in identifying adversaries and their interdiction at the different stages in the terrorist attack planning cycle. These challenges are particularly evident, as using a FAVBIED is essentially a publically accessible remote attack mechanism via a self-guided bomb whereby the adversary may be miles away when the action is initiated.

[236] Source: "JCAT Counterterrorism Guide for Public Safety Personnel," Office of the Director of National Intelligence, accessed January 13, 2019, https://www.dni.gov/nctc/jcat/index.html.

As seen in Figure 12, components of the terrorist planning cycle fit within the context of the fully autonomous vehicle mitigating strategy loop touchpoints of *before, during*, and *after*. Therefore, the strategy of utilizing dual-purpose technologies to mitigate the threat of FAVBIEDs blends within current terrorism modalities.

Before a FAVBIED attack, terrorists will typically identify a primary target, conduct intelligence and surveillance, finalize what they are attacking, conduct pre-attack surveillance, plan, and rehearse the attack. Although the FAV itself may not be the mechanism of destruction at this point, it does exhibit qualities preferential to threat actors who would prefer anonymity and a low profile during these stages. FAVs are partly being explored for their connection to the IoT that may allow the identification and monitoring of persons of concern. Although not necessarily actionable, taken in conjunction with other data, FAV use may help to paint a higher-level picture regarding threats that bear further inquiry and a relative determination of urgency.

During a FAVBIED attack, at times, the threat could potentially be mitigated via direct law enforcement intervention with the assistance of private partners. Analytical models can be developed where algorithms used in conjunction with subject matter experts can evaluate multiple indicators to spot a pending threat. FAVs that can be directed remotely may be diverted to safer locations or simply stopped for securement pending law enforcement action.

After a FAVBIED attack, many of the same metrics available *before* an attack will then be available for a more focused analysis as the terrorist is pursued. Data connectivity over multiple platforms, blending with information from FAVs, may be synthesized for investigative purposes. The speed and accuracy in which data synthesis occurs will have a direct impact on the investigative outcome. Additionally, the inversion mental model can be embraced as Carl Jacobi related, “it is in the nature of things that many hard problems are best solved when they are addressed backward.”[237]

[237] “Inversion: The Power of Avoiding Stupidity,” *Farnam Street* (blog), October 28, 2013, https://fs.blog/2013/10/inversion/.

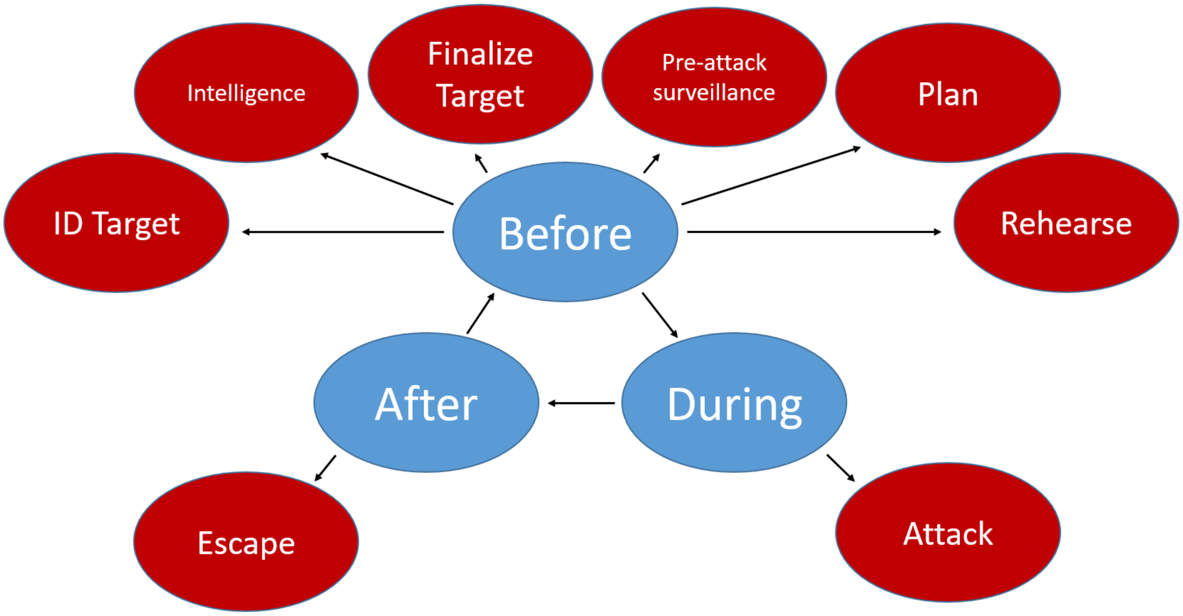


Figure 12. Fully autonomous vehicle-borne improvised Explosive Device Mitigating Strategy Loop with Terrorist Planning Cycle Augment

D. SCENARIOS

Imagination is a powerful tool. Generations can be inspired by positivity and families can experience unforgettable joy, such as when visiting the fantastical land imagined by Walt Disney. Conversely, some are guided by darkness and warped rationales that represent the personification of evil where death is the intended outcome. By drawing inspiration from prior appalling events and imagining them in an alternate setting via scenarios, it is the sincere desire of this author to impact the discussion on FAVBIED mitigating strategies positively. Perhaps proactive engagement resulting from horrific experiences can be a positive outcome in contrast to gratuitous "thoughts and prayers." For the purposes of this discussion, three hypothetical scenarios are presented to highlight potential nefarious activities that can impact homeland security as FAVs are deployed throughout the United States. When reading these scenarios, ask if other victims could be substituted into each example? Section E. Analysis, "What just happened?," addresses the attacks; i.e., how they were planned and provides details on the use of technology.

1. Is It a Cat or a Bomb?

Judge Hammer was overseeing the murder trial of a notorious cartel leader. As she was efficient with her time, Judge Hammer used her FAV to commute to work and review court briefs amongst her other preparations for the day's proceedings. The judge also used her FAV on occasion to run errands. On this day, Judge Hammer was working from home and placed her cat, Mr. Whiskers, in his cat carrier, and buckled it into her FAV. Judge Hammer then directed the FAV to transport Mr. Whiskers to the kitty day spa for his weekly pampering. The kitty day spa employees would receive a text from the FAV as it pulled into the designated parking space in front of their business and retrieve Mr. Whiskers for his spa day. The employees would then text Judge Hammer when Mr. Whiskers arrived safely and Judge Hammer would direct the FAV home if needed. Meanwhile, Judge Hammer continued working from home as she was engaged with trial preparations. Later the same day, Mr. Whiskers was being returned home after a good pampering. The FAV pulled up to the security gate for Judge Hammer's neighborhood and was waved through by the local security guard having recognized the vehicle and Mr. Whiskers' cat carrier. Having received a text about the pending arrival of her FAV, Judge Hammer was waiting in her front driveway for Mr. Whiskers. The FAV pulled into the driveway. As Judge Hammer opened the car door to retrieve Mr. Whiskers, the vehicle exploded and she was killed. Mr. Whiskers miraculously survived the blast and was retrieved from a nearby tree with the assistance of a local firefighter.

2. Next Level Hooligan

Super fan Rowdy Chucklehead was absolutely pissed. Once again, his favorite soccer team, Blue City, lost to their arch rival, United Princes. Of course, it was yet another blown call by a referee and the television pundits covering his team confirmed these suspicions by showing several not-so-conclusive replays.

For the next several weeks, Rowdy continued to read news articles, blogs, social media, and the Blues *Down for the Cause* super fan club emails and posts discussing the fact that not only was it a blown call, but it was probably a conspiracy between the referees, the Princes', the league, and a secretive sheik from the United Arab Emirates to ensure Blue City does not win another championship ever again.[238] What Rowdy did not realize is all the algorithms for accessing his information were refined to impact his emotions.[239] By getting Rowdy upset and angry, he would spend hours clicking through the internet.[240] The information Rowdy was receiving actually represented only a fraction of the actual population in his community heavily penetrated by social media.[241] It turns out Rowdy had isolated himself in an echo chamber of hate and violence.

Rowdy was truly *Down for the Cause* and decided that, if his team were ever to have the chance at winning a championship again, something had to be done. Watching never-ending visuals of Princes fans celebrating their win over his Blues was unbearable. Rowdy decided the smug Princes fans needed to be taught a lesson. He used an online street view program and examined the surroundings around The United Princes stadium. The United Princes team web page even had a map of the facilities including parking and drop off points for FAVs located conveniently next to the fan entrance security cues. Then, a picture of a Princes fan's tattoo meme celebrating the controversial victory went viral and Rowdy was incensed.

The target was finalized. Rowdy had to make a BIG statement and researched via the internet how to make a bomb. He obtained raw materials and planned to fill two sizeable duffle bags with explosive materials, place them in the trunk of a FAV taxi service, and send it to the United Princes stadium for payback at their next home game. Rowdy used his smartphone app and called for a FAV taxi with the push of a button for a test drive where he timed the route to the stadium and viewed the interactive map on his phone display to compare it with his real-time progress to the drop off point.

[238] Farnam Street, "Complexity Bias."

[239] Amanda Taub and Max Fisher, "Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests," *New York Times*, sec. World, August 23, 2018, https://www.nytimes.com/2018/08/21/world/europe/facebook-refugee-attacks-germany.html.

[240] James Temple, "Evidence Is Piling up That Facebook Can Incite Violence," *MIT Technology Review*, August 21, 2018, https://www.technologyreview.com/the-download/611920/evidence-is-piling-up-that-facebook-can-incite-racial-violence/.

[241] Karsten Müller and Carlo Schwarz, "Fanning the Flames of Hate: Social Media and Hate Crime," *SSRN Electronic Journal* 373 (May 2017): 5, https://doi.org/10.2139/ssrn.3082972.

The day of the big game arrived. Rowdy called for a FAV taxi and quickly loaded the sizeable duffle bags into the vehicle trunk once it arrived. News agencies later that day reported that at approximately 10 minutes prior to the start of the game at United Princes stadium, a FAVBIED exploded that killed 22 people and injured an additional 84.

3. Comic-Con Gone Wrong

Electricity was in the morning air as throngs of people from all ages gathered outside the convention center entrance to their cities' Comic-Con. Many of the children and adults were dressed in elaborate costumes paying homage to the fantastical. This fun-loving collective entered the event and started their day of seminars, contests, photo opportunities, shopping, and camaraderie.

Later in the early evening, the Comic-Con attendees started gathering around one another's phones in an attempt to understand what was happening throughout their city. Apparently, a car had caught fire on a local freeway and exploded. One vehicle would not have raised any eyebrows. However, then two more cars actually exploded in different locations on city surface streets near an entertainment district. One of the car explosions in the city was caught on video that quickly went viral. The echoes of emergency vehicles driving at breakneck speeds with their sirens screaming resonated throughout the city. Every local news agency was scrambling to cover the mayhem live to report about what they knew and pontificating about what they did not.

What 12 Deadpool, eight Spiderman, three Borg, Gamora, and countless Stormtroopers, along with all the other attendees, did not realize was something was horribly wrong right where they were. Fifteen minutes prior to the first vehicle explosion on the freeway, three attendees arrived, each in their own FAV ride-share and dressed in tactical cosplay gear resembling Umbrella Corporation soldiers. The problem is that their costumes were not just pretend. While the surface streetcars were exploding in the entertainment district, the cosplay soldiers drew their weapons, and in character, started killing as real world first person shooters.[242]

E. ANALYSIS

The intent of this section is to allow the reader to view the scenarios with a homeland security perspective and visualize lessons learned through the aforementioned methodologies. These scenarios are intentionally not comprehensive but merely offer highlights about the immediate aftermath; identify real-life examples to facilitate understanding of applicability and suggest FAV technologies that, via public private partnerships, may help to mitigate the threat of FAVBIEDs.

1. Is It a Cat or Bomb?

What just happened?

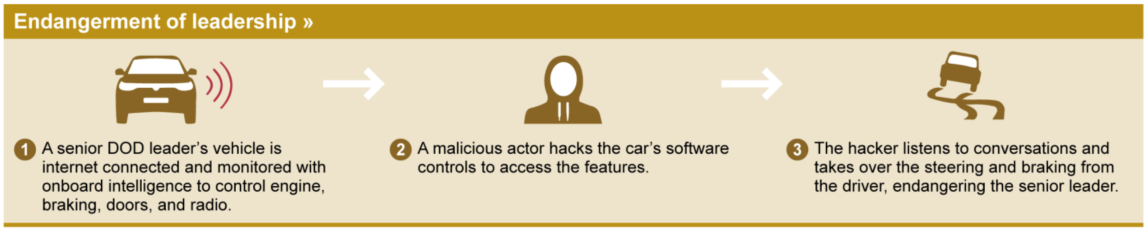
The investigating law enforcement agency retrieved the EDR from what remained of the FAV and eventually determined the vehicle, after having been hacked, inexplicably stopped for approximately two minutes while driving to the home of Judge Hammer and during this time, the FAV was likely implanted with an IED designed to explode when the car door was opened.

a. Terrorism Impetus

Connectivity to the IoT is an identified security challenge. The Government Accountability Office in *Report to Congressional Committees: Internet of Things, Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD* recognized a similar scenario where FAV vulnerabilities could result in endangering lives, as illustrated in Figure 13.[243]

[242] Dave Grossman, "Are Video Games Breeding an Assassination Generation?," Daily Beast, November 18, 2016, https://www.thedailybeast.com/articles/2016/11/18/are-video-games-breeding-an-assassination-generation.

[243] Government Accountability Office, *Report to Congressional Committees, Internet of Things, Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD*, GAO-17-668 (Washington, DC: Government Accountability Office, 2017), 14, https://www.gao.gov/assets/690/686203.pdf.


Endangerment of leadership »

1 A senior DOD leader's vehicle is internet connected and monitored with onboard intelligence to control engine, braking, doors, and radio.

2 A malicious actor hacks the car's software controls to access the features.

3 The hacker listens to conversations and takes over the steering and braking from the driver, endangering the senior leader.

Figure 13. One Example from the Notional IoT Scenarios Identified by the Department of Defense[244]

Attacking public officials is not new. Although not commonplace, the United States does have a history of judiciary being victims of violent crime in the course of their duties including being murdered by contract killers and mail bombs.[245] Unfortunately, to the south of the United States, the circumstances are much direr for politicians in Mexico, as over 100 were killed prior to the country's recent election that largely resulted from the national failure to combat organized crime.[246]

The FBI is also worried FAVs can become self-guided bombs.[247] Countries developed GPS to be used with precision guided munitions and now FAVBIEDs using this same technology will soon be available to everyone.[248] FAVs will also pose a new challenge with how protective forces maintain physical security. How will people be able to identify FAV threats for the purposes of maintaining a physical security perimeter?[249]

[244] Source: Government Accountability Office, 14.

[245] "Judges Targeted Fast Facts," CNN, updated April 18, 2018, https://www.cnn.com/2013/11/04/us/judges-targeted-fast-facts/index.html.

[246] Natasha Turak, "More than 100 Politicians Murdered in Mexico Ahead of Election," CNBC, June 26, 2018, https://www.cnbc.com/2018/06/26/more-than-100-politicians-murdered-in-mexico-ahead-of-election.html.

[247] Mary Beth Griggs, "The FBI's Next Worry: Self-Driving Car Bombs," *Smithsonian*, July 17, 2014, https://www.smithsonianmag.com/smart-news/fbi-worried-self-driving-cars-could-be-used-bombs-180952082/.

[248] Jeffrey W. Lewis, "A Smart Bomb in Every Garage? Driverless Cars and the Future of Terrorist Attacks," National Consortium for the Study of Terrorism and Responses to Terrorism, September 28, 2015, http://www.start.umd.edu/news/smart-bomb-every-garage-driverless-cars-and-future-terrorist-attacks.

[249] Frederic Petit et al., *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability* (Lemont, IL: Argonne National Laboratory, 2013), 7.

This issue will be even more challenging as package delivery services start utilizing FAVs for delivery services. Consider Amazon, currently a customer can have a package delivered to a local locker, typically located in a supermarket, or dropped off on their front doorstep.[250] Imagine customers having the option to select an even quicker home delivery method for receiving a package delivered via FAV where they just step out front to obtain the package after receiving a text notification. This concept would merely be a FAV extension of Amazon Flex, which is, "an Uber-like crowdsourced delivery service, now available in more than 50 U.S. markets, which utilizes approximately 100,000(!) drivers."[251] Imagine the disruption to legacy delivery companies, such as FedEx and UPS, when people now have access to a revenue stream by having their FAVs provide Amazon deliveries while they sleep![252]

b. The FAVBIED Mitigating Strategy Loop

Before the assassination of Judge Hammer occurred, indicators could have presented themselves. Connectivity of FAVs when combined with biometric identification might have been able to identify associates of the person on trial and determine they were worth watching. Should these associates have been in proximity to the Judge's residence, work parking, or other locations associated with her daily living patterns, red flags might have possibly been raised. If these associates had used FAVs for any of their pre-attack surveillance or rehearsal, then another opportunity for analytics could have resulted to recognize something of concern.

On the day of the event or *during*, the FAV was hacked. This hacking should have caused an immediate tampering reporting and the FAV should have gone into some sort of safe mode whereby it would need an assessment, either remotely via a system check and possibly physically via law enforcement or other identified specialist. The vehicle would also normally require some sort of biometric identification to access the interior.

[250] Itamar Zur, "Make No Mistake: Amazon Is Going to Take on Delivery Behemoths FedEx and UPS," *Medium* (blog), May 17, 2018, https://medium.com/@itamarzur/make-no-mistake-amazon-is-going-to-take-on-delivery-behemoths-fedex-and-ups-d047cf6b6b0c.

[251] Zur.

[252] Zur.

The compromised FAV should have some sort of remote identification communicated to the security officer working the gate to the neighborhood. The officer could have then determined something was not right and investigated the circumstances further. The same is true as the vehicle parked in the Judge's driveway. As she went to open the door, the FAV would have biometrically identified her and had another opportunity to communicate the vehicle had been tampered with, that additional cargo was in the vehicle that was not part of the original manifest (Mr. Whiskers), the overall weight of the vehicle was off, or other inconsistencies that differ from prior use tendencies.

After the event, the vehicle did have mechanisms in place for follow-up including the data in the "black box" and all the recent information uploaded during normal operations resulting from interconnectivity. The hacked code and the mechanism by which the system was penetrated, combined with the location where the breach occurred, would be particularly valuable.

2. Next-Level Hooligan

What just happened?

The investigating law enforcement agencies utilized the FAV's interconnectivity with both the surviving black box and cloud-based activity data retained where they immediately determined who summoned the FAVBIED and directed it to the stadium. Analytics were able to determine Rowdy had previously used a FAV to travel the exact same route. Other cyber crumbs to Rowdy's FAV activities connected him to the bomb making supplies. His internet activities conducted in a FAV ride-share coinciding with the routes traveled clearly showed his motivations and were further evidence of his culpability.

a. Terrorism Impetus

Research shows that throughout recent history many sporting events have experienced bombings. Both the 2008 Sri Lanka Marathon and 2013 Boston Marathon experienced mass deaths and casualties resulting from bombs.[253] Soccer sporting events also have a distinct history of being bombed. The Irish Republican Army in 1996 blew up a cargo van with a 3,300-pound bomb in a shopping center during the European Football Championship.[254] Eta, a Basque separatist group, exploded a car bomb in 2002 outside Real Madrid's stadium during the semi-final for the European Champions League.[255] More recently, in 2015, a triple suicide bombing occurred in Paris, France outside the Stade de France stadium hosting a soccer friendly match between Germany and France.[256]

VBIED attacks have occurred throughout the world with severe consequences. In the United States, two significant VBIED attacks have occurred. These attacks are obvious examples of damage and death that can occur that may be compounded should the equivalent delivery mechanism (vehicle) and explosive size be used in a sports venue setting. On February 26, 1993, an approximately 1,200-pound bomb VBIED detonated in the World Trade Center underground garage.[257] On April 19, 1995, an approximately 4,000-pound bomb VBIED detonated outside the Alfred P. Murrah Federal Building located in Oklahoma City.[258] Extrapolating from these two examples leads to the needed understanding of *standoff distance*, which is defined as, "the distance between the explosive threat location and the nearest building element that requires protection."[259]

Lastly, although not an IED, on January 16, 2001, a semi-truck combination vehicle weighing over 78,000 pounds was driven into the south entrance of the restored

[253] Jane J. Lee, "7 Other Sports-Related Attacks," National Geographic News, April 16, 2013, https://news.nationalgeographic.com/news/2013/03/130415-sports-marathon-olympics-bombers-culture/.

[254] Lee.

[255] Giles Tremlett and Michael Walker, "Football Fans Flee Madrid Blast," *Guardian*, May 2, 2002, sec. World news, https://www.theguardian.com/world/2002/may/02/football.spain.

[256] David Conn, "Dortmund Attack: How Soccer Has Became a Target of Terrorists," *The Irish Times*, April 12, 2017, https://www.irishtimes.com/sport/soccer/champions-league/dortmund-attack-how-soccer-has-became-a-target-of-terrorists-1.3046763.

[257] Tom Hays, "AP Was There: The 1993 Bombing of the World Trade Center," AP News, February 26, 2018, https://apnews.com/f4f1fd2b2d4b4a17b94ca7183fb65ba4.

[258] Michael R. Bloomberg, Raymond W. Kelly, and Richard A. Falkenrath, "New York City Police Department, Engineering Security: Protective Design for High Risk Buildings," 105 (2009): 12.

[259] Bloomberg, Kelly, and Falkenrath, 15.

side of the California State Capitol.[260] The semi's fuel tanks exploded and subsequent repairs to the State Capitol cost over $13.5 million dollars.[261] The official California Highway Patrol report indicated the truck drove into the Capitol at 46 mph.[262]

b. The FAVBIED Mitigating Strategy Loop

Before the incident, many described opportunities (aka bread crumbs) left by Rowdy resulted, where if analytical tools had existed and been appropriately refined, could have provided indicators that something was amiss. However, one of the challenges was that Rowdy was working by himself. Lone wolf terrorists are hard to detect unless fused with intelligence and an understanding of the radicalization process.[263]

During the incident, having an appropriately designed standoff distance for the FAV drop-off location would have helped minimize the deaths and injuries. It has also been considered that FAV ride-share vehicles should drop-off in a different location from where riders are picked-up. Additionally, the venue could also have an operational plan, whereby during designated events, no occupied or unoccupied delivery vehicles would be admitted on the premises. Geo-fencing could also restrict vehicle access to different areas of the event venue either permanently or on an "as-needed" basis.[264] The FAV itself could have had analytics that detected a possible issue with having a ride-share request to a stadium on a game day result in transporting cargo as opposed to occupants.

After the incident, the scenario description indicated several mechanisms where follow-up led to the identification and apprehension of Rowdy.

[260] "FROM THE ARCHIVE: Truck Intentionally Strikes California Capitol, Bursts into Flames," CBS Sacramento, 13, April 18, 2016, https://sacramento.cbslocal.com/2016/04/18/from-the-archive-truck-intentionally-strikes-california-capitol-bursts-into-flames/.

[261] Cathy Locke, "Ask Sacto 911 Crime Q&A: What Happened to Man Who Crashed Semi Truck into State Capitol in 2001?," *Sacramento Bee*, January 2016, https://www.sacbee.com/news/local/crime/article 53249580.html.

[262] Locke.

[263] Mark Hamm and Ramon Spaaj, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies* (Terre Haute, IN: Indiana State University, 2015), 13.

[264] Eleonora Malacarne, "Vehicle Tracking Geo-Fencing: UK Exploring Technology against Terrorism," Transpoco, August 10, 2017, https://www.transpoco.com/blog/vehicle-tracking-geo-fencing-uk-exploring-technology-against-terrorism.

3. Comic-Con Gone Wrong

What just happened?

Due to the close proximity of all the explosions, law enforcement was able to respond quickly to the active shooters. An off-duty officer immediately engaged the threat and neutralized one of the perpetrators.[265] Seeing that the first active shooter was quickly confronted and killed, the remaining two active shooters turned their weapons on themselves and committed suicide.[266]

a. Terrorism Impetus

On July 20, 2012, a massacre occurred at a movie theater showing *The Dark Knight Rises.*[267] The attack was carried out with an arsenal of weaponry and had been planned down to the minute details.[268] During the movie, the mass murderer stepped out of the movie theater to don tactical gear and obtain weapons and then returned to kill.[269] Police apprehended the murderer behind the movie theater with an assault rifle, shotgun, and a handgun.[270]

Starting on November 26, 2008, a major terrorist event perpetrated by a terrorist group based in Pakistan occurred in Mumbai, India.[271] During the course of this event, attackers entered the city harbor by boat and some of them used taxis to travel to different

[265] Dan Marcou, "Armed in America: It's Not Easy Being a Retired Cop," PoliceOne, November 14, 2018, https://www.policeone.com/gun-legislation-law-enforcement/articles/482065006-Armed-in-America-Its-not-easy-being-a-retired-cop/.

[266] Scott A. Bonn, "The Mass Shooting-Suicide Connection," *Psychology Today*, February 22, 2018, https://www.psychologytoday.com/blog/wicked-deeds/201802/the-mass-shooting-suicide-connection.

[267] Julia Jacobo, "A Look Back at the Aurora, Colorado, Movie Theater Shooting 5 Years Later," ABC News, July 20, 2017, https://abcnews.go.com/US/back-aurora-colorado-movie-theater-shooting-years/story?id=48730066.

[268] Shelley Jofre, "The Batman Killer—A Prescription for Murder?," BBC News, July 26, 2017, https://www.bbc.co.uk/news/resources/idt-sh/aurora_shooting.

[269] Jacobo, "A Look Back at the Aurora, Colorado, Movie Theater Shooting 5 Years Later."

[270] Jacobo.

[271] Angel Rabasa et al., *The Lessons of Mumbai* (Santa Monica, CA: RAND, 2009), 1.

parts of the city to plant bombs within the two vehicles.[272] After exiting the taxis, the bombs remained and later exploded, as the devices were on timers.[273] The bombs were placed under the taxi driver's seats that killed the drivers and occupants while contributing to the chaos with multiple simultaneous attacks occurring throughout the city of Mumbai.[274]

b. The FAVBIED Mitigating Strategy Loop

Before the incident, many opportunities for analytics might have been available to identify the attackers while they were conducting *pre-attack surveillance* while using FAVs and biometrics connecting them to possible internet activity. This same methodology of using biometric identification with analytics could also apply during the *rehearsal* phase.

During the incident, it is a possible that the vehicles may have been equipped with cargo detection capabilities and determined something was wrong. As the passengers would have been identified, this data would have been available to FAV public and private partners. This information, combined with three vehicles stopping at the same location, in addition to starting at a similar location, with all them having unintended cargo, would likely have been a cause for concern. After the explosions, data would have been available to identify the vehicle users and where they were last seen, likely including video images from FAV exterior and interior cameras showing the attacker's tactical attire. After the first freeway explosion, it is also possible that a first responder may have detected explosive material and immediately initiated some sort of protocol for all FAVs in the region that may have experienced similar suspicious circumstances and remotely sequestered them for law enforcement follow-up.

[272] "How 26/11 Mumbai Attack Happened in 2008: From First Eyewitness to Kasab," India Today, November 26, 2017, https://www.indiatoday.in/india/story/how-2611-mumbai-terror-attack-happened-in-2008-from-first-eyewitness-to-kasab-1094473-2017-11-26.

[273] Soumyajit Majumder, "26/11 Mumbai Attacks Anniversary: A War Waged against India," NDTV, November 25, 2017, https://www.ndtv.com/mumbai-news/26-11-mumbai-attacks-anniversary-a-war-waged-against-india-1779783.

[274] Dhanya Nair et al., "Tracing the Terror Route," The Indian Express, Journalism of Courage Archive, December 10, 2008, http://archive.indianexpress.com/news/tracing-the-terror-route/396335/1.

After the incident, substantial FAV data “bread crumbs” would have been available for investigative follow-up. After a thorough investigation, the lessons learned could be applied to the FAV monitoring analytics and allow refinement to mitigate the use of FAVs as VBIEDs further.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A MATTER OF PERSPECTIVE

Mitigating the threat of FAVBIEDs will involve the coordination of numerous stakeholders working together to protect their mutual constituency, the American public. Part of the challenge is realizing that all stakeholders bring their own unique perspective to the conversation. The public does not care about jurisdictional boundaries amongst government agencies. When the public has a problem, they just want it solved. Similar thoughts resonate about tragedies involving private industry. When a commercial airline crashes, the public wants two things: (1) accountability because someone needs to be blamed, and (2) assurances that something is being done so it will not happen again. To this end, this thesis looks to explore what needs to be considered for FAVBIED mitigating strategy implementation, priorities, incentives, and gaps in knowledge.

A. RISK ASSESSMENT

The imperative for FAV manufacturers and the homeland security enterprise to work collaboratively toward ensuring public safety cannot be understated. When the FAVs operate as intended, and are not subjected to nefarious misappropriations, then their operation can be considered a success. The converse is also true in that should a FAV be used as a VBIED, then it will be considered a failure. This discussion seeks to communicate the nature of FAVBIED risk in the context of the *Risk Management Process.*[275]

In establishing context for risk to be *identified*, it is necessary to recognize both internal and external factors that may impact a successful use of FAVs in the United States.[276] Internally, financial resources and investment opportunities are required for this industry to conduct R&D. R&D needs to be shepherded in a physical environment conducive to the form of proper facilities and a productive forum for employees. Internal risk could also involve potential intellectual property theft via employees (or intellectual property theft externally via espionage). Employees may also fail to perform their duties,

[275] ECRRN European Cyber Resilience Research Network, "6 Steps Risk Management Approach."

[276] ECRRN European Cyber Resilience Research Network.

which may also have a negative impact on the brand, developmental progress, and public acceptance of this emerging technology.[277] External factors, or outside influences, will also have an impact on the successful deployment of FAVs. Competition, legal constraints, and the overall economy all have an impact. However, two major external concerns are technology, with how it can be dual-use in nature for unintended bad purposes, as well as political environments, with how terrorism within the context of social identity theory can be seen as a means of communication by those who perceive themselves as being marginalized.[278] The remainder of this risk discussion looks to build upon external factors contributing to the threat of FAVBIEDs via a risk management process.[279]

The external risk being faced is the use of a FAV as an IED. Different strategies, when combined, can help mitigate the threat of them being used as a FAVBIED. However, short of not allowing FAVs to exist, no single solution would eliminate this risk. Options for mitigating the threat include:

- implementing technological and physical constraints on where the actual vehicle is allowed to travel
- biometrics and other markers for user identification
- internal vehicle capabilities that can identify intended or unintended cargo or occupants
- internal vehicle system checks to identify unauthorized computer system access in conjunction with a means to report incursions
- a mechanism for external vehicle control up to and including redirection and shut-down

[277] Garsten, "Sharp Growth in Autonomous Car Market Value."

[278] Saul McLeod, "Social Identity Theory," SimplyPsychology, 2008, https://www.simplypsychology.org/social-identity-theory.html.

[279] ECRRN European Cyber Resilience Research Network, "6 Steps Risk Management Approach."

Although not a comprehensive list, it is intended as a starting point for discussing which mitigating strategies can be realized.

The impact of the successful use of a FAVBIED could be immense. Even if the total amount of deaths were minimal, the fear generated would be substantial. Additionally, once the proverbial "genie in a bottle" is let out, it can never be put back in. That being said, once a FAV is used as an IED, the expectation is that others will follow suit, as asymmetrical means to conduct violence have tactical advantages for terrorists. Only through a combination of different strategies can this risk be minimized, as opposed to controlled, reversed, or avoided.[280] As a whole, the different stakeholders involved in this discussion would classify the risk of a FAVBIED as "terrorism."

1. Risk Assessment

Risk assessment seeks to evaluate incident exposure from the viewpoint of probability while also considering consequences per event.[281] Probability involves evaluating data to make a determination on the likelihood of occurrence. Given that FAVs are not greatly available to the general public at this time, determining a probability may be problematic. However, when extrapolating experiences with the growth of the sUAV market, and subsequent dual-technology uses by terrorists that have occurred throughout the world, it would be reasonable to project that as FAVs become increasingly available, the likelihood of misuse would increase. The consequences of a successful FAVBIED use would be significant. They would range from the following:

- injuries and loss of life
- massive law enforcement investigations
- internal or international conflict (war) should the terrorist be a member of a group or nation
- economic losses from individual brand and FAV industry degradation

[280] ECRRN European Cyber Resilience Research Network.

[281] ECRRN European Cyber Resilience Research Network.

- loss of trust and fear associated with FAVs
- loss of transportation network productivity as FAVs are evaluated and possibly subject to government "never again" mandates

Conversely, it also needs to be recognized that the impact of a FAVBIED detonation may be minimal, as some horrific events, such as K-12 school shootings, have resulted in nominal strategic responses as the total number of children injured and killed annually continues to trend upward.[282]

2. Risk Control

When considering risk control measures, this discussion needs to acknowledge that the priority of this thesis is mitigating the threat of FAVBIEDs. When looking at the spectrum of FAV threats, having FAVBIEDs could be on the high end of negative outcomes for an individual vehicle. However, as FAVs are interconnected via the IoT, much worse can happen. As this thesis is considering a singular FAVBIED risk, risk control measures explore *options* to this singular threat.[283] Avoiding this risk is not feasible, as FAVs will be made available in the foreseeable future. Implementing FAVBIED strategies could help to change the likelihood of this risk. Restricting the environment, as in where FAVs are allowed to drive in proximity to targets of opportunity, may minimize the consequences of a successful FAVBIED deployment. The most powerful *option* would be to share the risk amongst different stakeholder groups. Sharing risk would incentivize the need for private public partnership collaboration and ongoing interconnectivity, as they all want to ensure the safety of the public.

The impetuses of risk controls implementation is to establish a mechanism for accountability through delineating responsibility, providing structure, and articulating procedures.[284] Responsibility starts with the need for private industry involvement in the development, manufacture, and ancillary use of FAVs to collaborate with the homeland

[282] David Riedman, "Incidents by Injured and Killed Annually," *K-12 School Shooting Database* (blog), August 25, 2018, https://www.chds.us/ssdb/incidents-by-injured-killed-annually/.

[283] ECRRN European Cyber Resilience Research Network, "6 Steps Risk Management Approach."

[284] ECRRN European Cyber Resilience Research Network.

security enterprise for implementation of FAVBIED mitigating strategies. Failure on the part of private industry to contribute voluntarily and meaningfully to mitigating strategy development and implementation would be their exclusive burden to bear should a catastrophe occur. Ongoing accountability will involve public private partner relationships leveraging FAV interconnectivity with different resources, including government databases and mechanisms to allow for real-time notifications should analytics detect actionable circumstances. The goal is to put both private interests and government interests in a position to succeed for the long term. As this technology evolves, other challenges will arise that have yet to be conceptualized and this initial foundational effort will allow for the continued safety of the public.

3. Monitoring and Reviewing

Monitoring and reviewing involves developing procedures and processes to audit activities; thereby, to ensure things are working effectively and adjust or improve if needed for quality control purposes.[285] The intent not only is to put systems in place, but to be forward thinking and establish an adaptable environment for the long term. The threat of FAVBIEDs will not simply disappear over time. Throughout history, people have been very creative with new technologies and their unintended dual-use of killing one another.[286] Monitoring mechanisms are absolutely necessary for the long-term success of the proposed public private partnership. As Peter Drucker wrote, “What gets measured gets managed.”[287] Implemented systems need to include analytics to measure the volume of suspicious circumstance notification activity with the actual outcomes to allow for system refinement and identify gaps in capabilities and resources, both physical and technological, across the public private partnership homeland security spectrum.

[285] ECRRN European Cyber Resilience Research Network.

[286] Koos van der Bruggen, “Possibilities, Intentions and Threats: Dual Use in the Life Sciences Reconsidered,” *Science and Engineering Ethics* 18, no. 4 (December 2012): 742, https://doi.org/10.1007/s11948-011-9266-2.

[287] Larry Prusak, “What Can’t Be Measured,” *Harvard Business Review*, October 7, 2010, https://hbr.org/2010/10/what-cant-be-measured.

B. INCENTIVES

Manufacturers have incentives to minimize the occurrence of their FAVs being used as car bombs. In an economic environment, product preference impacts demand in the market place. The success of FAVs will be intertwined with public acceptance. Public acceptance will be impacted by a FAV's ease of use, availability, cost, personal safety, and overall public safety. Overall, a FAV manufacturers would not want their products to be associated with them being used as a VBIED. Harre-Young developed a "concept map" on generalized incentives to safeguard densely populated pedestrian areas from VBIEDs, some of which have been adapted and expanded upon for discussion in this section:[288]

Manufacturer incentives to protect FAVs have a benefit of reducing the risk of being used in an attack. Minimizing the propensity of a particular FAV to be used as a VBIED would result in possibly displacing the threat elsewhere or disincentivizing the attempt in the first place.[289] Hardening infrastructure is a common tactic to mitigate the threat of terrorism. For the purposes of a FAV, hardening would amount to making its use as a VBIED more challenging. This strategy would not eliminate the threat, but merely attempt to reduce the likelihood.

Reducing impacts of an attack will have several benefits. If an explosion occurs, fewer injuries result, less lives are lost, property damage is reduced, and damage to a manufacturer's reputation is minimized along with the overall impact to the FAV industry.[290] Some of the strategies referenced later in the Recommendations section will seek to keep FAVs out of crowed areas where fewer potential victims or targets are present. The cost of a successful deployment of a FAVBIED will include substantial brand degradation (loss of value) and likely result in increased regulatory mandates (increased manufacturing or compliance costs). As an example, much of the commercial

[288] Steven Nicholas Harre-Young, *The Relative Performance and Consequences of Protecting Crowded Places from Vehicle-Borne Improvised Explosive Device* (Loughborough, UK: Loughborough University, 2012), 126, https://dspace.lboro.ac.uk/2134/9757.

[289] Harre-Young, 125.

[290] Harre-Young, 128.

airline industry regulatory oversight has evolved as a mechanism to prevent tragedies from re-occurring.[291]

A competitive advantage could result from reducing the chances of a FAV being used as a VBIED, as the product could be perceived as being more valuable and the subsequent improvement of the products overall brand and value.[292] An example of a product being more secure by end users, and, in part, garnering a higher sales price point, would be iOS versus Android.[293] As the Apple iPhone is perceived to be, or actually is, more secure, customers may be drawn to the product, in part, because of this capability.[294] As Conroy et al. state, "Consumer product executives should consider viewing data privacy and security not just as a risk management issue, but as a potential source of competitive advantage that may be a central component of brand-building and corporate reputation."[295] FAV connectivity with the IoT is a safety issue. Simply put, if a phone is hacked, it is an inconvenience; if a FAV is hacked, it may harm "flesh and blood."[296]

C. RETURN ON INVESTMENT

Incorporating counter-terrorism measures into FAVs will be dependent, in part, on how much they will cost, as well as their ROI. The motivation behind this thesis is to promote mitigating strategies that incorporate both software and hardware that is, or is projected to be, integrated within FAVs that are dual-use in nature. In turn, the implementation of counter terrorism measures in FAVs will be much more palatable to

[291] David Nol and Barbara Peterson, "12 Plane Crashes that Changed Aviation," *Popular Mechanics*, August 4, 2017, https://www.popularmechanics.com/technology/aviation/crashes/10-airplane-crashes-that-changed-aviation.

[292] Harre-Young, *The Relative Performance and Consequences*, 128.

[293] Kari Paul, "Apple or Android? Here Is the Most Secure Phone You Can Get," MarketWatch, January 6, 2019, https://www.marketwatch.com/story/apple-or-android-here-is-the-most-secure-phone-you-can-get-2018-10-10.

[294] Simon Hill, "Android vs. IOS: In-Depth Comparison of the Best Smartphone Platforms," Digital Trends, January 17, 2019, https://www.digitaltrends.com/mobile/android-vs-ios/.

[295] Pat Conroy et al., "Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry," Deloitte Insights, November 13, 2014, https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html.

[296] Massimilia, "Connected, Self-Driving Cars."

private industry. In large part, much of what has been considered may be categorized as software development and can be incorporated in FAVs with their initial purchase and pushed out as system updates whenever needed to take advantage of vehicle connectivity. The exact cost of the software development would be nominal when compared to the physical and financial risk of a successful FAVBIED deployment to both a company's brand and the entire FAV industry, not to mention all the governmental expenditures. Would the governmental response to a successful FAVBIED deployment cost more or less than the $100 billion spent on protecting airports and air travel since the 9/11 attack?[297]

Lessons can be learned from protecting infrastructure from VBIEDs. As Cherry stated, "Because terrorist attacks are relatively rare and design elements to deter terrorism are very expensive, these design elements must serve multiple purposes in order to be justified."[298] Designing dual-use FAV elements from the outset could further decrease costs in the long term for the application of mitigating strategies. Analysis of potential threats could aid in designing mitigating capabilities and a joint effort with public private partnerships could be very constructive and cost effective from a ROI perspective. Communicating these needs is necessary to assist those tasked with developing and implementing infrastructure (in this case, FAVs) so informed decisions in the appropriate context can be made.[299]

[297] Barbara Peterson, "How Airport Security Has Changed Since 9/11," *Condé Nast Traveler*, September 10, 2016, https://www.cntraveler.com/story/how-airport-security-has-changed-since-september-11.

[298] Christopher Cherry, Anastasia Loukaitou-Sideris, and Martin Wachs, "Subway Station Design and Management: Lessons from Case Studies of Contemporary Terrorist Incidents," *Journal of Architectural and Planning Research* 25, no. 1 (Spring 2008): 88.

[299] Harre-Young, *The Relative Performance and Consequences*, 81.

V. MOVING FORWARD

A. CONCLUSIONS

With the development of the FAV in conjunction with the evolution of asymmetrical public safety threats, problems and solutions once inconceivable in past years are now commonplace and continued disruptive technologies can be expected to be dual-use when looking toward the future. Admittedly, without regulatory mandates for adoption, the incentive for FAV manufacturers to embrace and enact the proposed mitigating strategies is more a function of self-interest rather than altruism. Manufacture cost benefit analysis may indicate a course of action, or lack thereof, contrary to the best interests of public safety. As stated in a report to Congress, "According to DoD officials, there is little incentive for manufacturers to design security functions into the software or hardware of their products, resulting in little thought or effort given to security."[300] Overcoming short-term motivations and creating the need for action will be challenging as Kaplan and Mikes relate, "And many leaders have a tendency to discount the future; they're reluctant to spend time and money now to avoid an uncertain future problem that might occur down the road, on someone else's watch."[301]

As technology evolves, software platforms now include vehicles or "tin wrapped software."[302] In other words, FAVs can actually become safer over time as software updates are pushed out to consumers.[303] By building upon this concept, threat mitigation of FAVBIEDs can continually evolve as new countermeasures are developed and deployed. As the FAVBIED attacks have yet to occur in the United States (or the world), identifying FAV technologies, current and predicted, that are dual-use in nature will make it easier for manufacturers to justify implementing threat mitigation strategies. As vehicles move toward continuous connectivity with the IoT, much of what has been

[300] Government Accountability Office, *Report to Congressional Committees*, 12.

[301] Kaplan and Mikes, "Managing Risks."

[302] Danny Paez, "Tesla's Software-First Approach Foreshadows the Future of Cars," Inverse, December 2, 2018, https://www.inverse.com/article/51390-tesla-electric-cars-software.

[303] Paez.

discussed and proposed is based on software solutions. Having vehicle elements serving multiple purposes is a much more palatable solution than mandating potentially expensive hardware and will go toward a cooperative public private partnerships working to address FAV strategic issues.

As stated earlier, although self-driving cars will be available in the immediate future, Americans may be hesitant to purchase them.[304] FAVs will eliminate human error and have the ability to save lives.[305] Over 37,000 people died from fatal traffic collisions in the United States during 2017.[306] Fatal traffic collisions rarely make the news unless there are extenuating circumstances. However, just the threat of terrorism elicits a profound response from the U.S. population that drives a narrative whereby these attacks must be prevented.[307] This dichotomy between prioritizing fatal collisions versus the threat of terrorism makes for challenging circumstances in allocating finite resources and the impetus to develop and deploy new technologies in furtherance of homeland security.

FAVs will be interacting with the motoring public to some extent in the immediate future. With the advent of this new technology, benefits and drawbacks result. Drivers and society can benefit from a more efficient use of existing transportation infrastructure and these vehicles will likely save lives by eliminating human error, amongst other things.[308] As stated by Peter Cheney:

> After a lifetime of driving, repairing and studying automobiles, I have come to an unavoidable conclusion—we are the weakest link in a car. As car components go, human beings are deeply substandard—we have

[304] Garsten, “Sharp Growth in Autonomous Car Market Value.”

[305] Anderson et al., *Autonomous Vehicle Technology*, 4.

[306] Tim Condon, “Leading the Way to AV Safety,” *VIA Magazine*, 2019, 7.

[307] Brian Michael Jenkins, “Brian Jenkins: Terrorists Can Use Cars, Trucks and Vans to Kill Their Targets. What’s the Best Way to Keep People Safe?,” Fox News, last updated September 19, 2017, http://www.foxnews.com/opinion/2017/09/03/brian-jenkins-terrorists-can-use-cars-trucks-and-vans-to-kill-their-targets-whats-best-way-to-keep-people-safe.html.

[308] Anderson et al., *Autonomous Vehicle Technology*, 114.

> imperfect perception, we are ruled by emotion, and we vary wildly in quality.[309]

The implementation of autonomous vehicle technology will also be challenging, as demonstrated with the Tesla S, Jeep Cherokee, and Corvette hacking examples. As Herberger states, "Autonomous vehicles will likely usher in safer, more convenient and more efficient transportation options… but only if we do everything we can to keep them secure."[310]

A more cautionary perspective of FAVs is related by Clerkin who warns, "driverless vehicles could be used in a wide range of terrorism tactics, from acting as self-driving bombs to holding passengers hostage if hackers remotely seize control of a vehicle."[311] Jessica Stern, a terrorism analyst, relates terrorists seek "to hit targets that will make us maximally afraid, and inflict the maximum amount of humiliation."[312] Although the current use of VBIEDs in the United States is rare compared to other regions of the world, it would not be surprising to see an increase as FAVs are more user friendly for those with bad intentions not interested in pursuing martyrdom. One of the costs imposed by FAVs is simply that the technology is soon available to everyone.[313] According to Peter Singer, with his reference to "open source warfare," he articulates nation states will simply purchase off-the-shelf software and hardware, reconfigure them to their dual-use needs, and avoid decades of expensive R&D.[314] As a tangent to this

[309] Peter Cheney, "What's the Weakest Link in Your Car?," The Globe and Mail, July 31, 2013, https://www.theglobeandmail.com/globe-drive/culture/commuting/whats-the-weakest-link-in-a-car/article 13499431/.

[310] Herberger, "Why the Department of Transportation's Self-Driving Car Guidelines Aren't Enough."

[311] Clerkin, "How Will We Ensure Security in a Self-Driving World?"

[312] Counter Extremism Project, *Terror Targets in the West: Where and Why* (New York and London: Counter Extremism Project, n.d.), accessed January 21, 2019, https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/CEP_Terror_Targets.pdf.

[313] Lewis, "A Smart Bomb in Every Garage?."

[314] Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009), 240.

topic, securing IoT connected devices from terrorists has led to the development of a threat analysis team sponsored by the Department of Justice (DoJ).[315]

B. RECOMMENDATIONS

The development and implementation of FAVBIED mitigating strategies raises the prospect of synergistic opportunities amongst vehicle manufacturers and the homeland security enterprise while improving public safety and enhancing of the overall transportation network experience. When considering mitigating strategies for FAVBIEDs, it needs to be noted that this thesis was intentionally constrained to decreasing the likelihood of one particular kind of terrorist activity, blowing up a fully autonomous car. Therefore, recommending strategies for consideration needs to be viewed in the light of the many other bad things that can and will likely happen with regard to the mass development and deployment of FAVs. Many of these recommendations will help not only to mitigate the threat of FAVBIEDs, but also help to minimize the occurrence other FAV threats as well. The following recommendations are technological solutions that should be implemented, proactively, to reduce the threat of FAVBIEDs.

1. FAVs Need to Have Constraints on Where They are Allowed to Drive

This need will be met through a combination of technological applications. When looking at parallel technologies, it has been learned that sUAVs can have airspace access restricted via geo-fencing. With thousands of locations already restricted due to geo-fencing worldwide where DJI sUAVs are not allowed to fly except in circumstances where the manufacturer allows for specific exemptions, such as authorizing first responders on a case-by-case basis, the same concept can be applied to FAVs.[316] As an example, FAVs could be prohibited from driving on California State Capitol grounds, as to avoid the circumstances experienced in 2001 when a big rig rammed the historic

[315] Dustin Volz, “Justice Dept. Group Studying National Security Threats of Internet-Linked Devices,” *Reuters*, September 9, 2016, https://www.reuters.com/article/us-usa-cyber-justice/justice-dept-group-studying-national-security-threats-of-internet-linked-devices-idUSKCN11F2FP.

[316] DJI Official, “DJI Introduces New Geofencing System for Its Drones.”

building and caught fire.[317] The United Kingdom is considering using geo-fencing and the Swedish government stated, "geo-fencing was a technological solution to enable only authorized vehicles to be driven within a geographically defined area."[318] In addition to geo-fencing, the vehicle's sensor systems could have the ability to recognize other prohibited FAV activities to include the ability of a FAV to recognize bike path configurations and prevent circumstances similar to what happened in New York when a rental truck driver intentionally struck and killed several people.[319] Jason Hanna commented on a Transportation Security Administration (TSA) memorandum asserting that terrorist groups would "continue to encourage aspiring attackers to employ unsophisticated tactics such as vehicle-ramming, since these types of attacks minimize the potential for premature detection and could inflict mass casualties if successful."[320] See Figure 14 for an image of ISIS propaganda.

Consideration should be given to programming stand-off distances to locations if possible, as the distance between a target and the bomb is an important factor.[321] However, it should be noted that when programming vehicle analytics and considering acceptable actions, ethical challenges will also arise. For instance, if a FAV is programmed not to strike pedestrians, circumstances may present themselves, as in the classic oversimplified *Trolley Problem* where a decision will need to be made about prioritizing the life of the pedestrian(s) versus the life of the vehicle occupant(s), which is beyond the scope of this discussion.[322] However, discussion has also been raised regarding the development of analytics that will presume to detect and even predict

[317] CBS Sacramento, "FROM THE ARCHIVE: Truck Intentionally Strikes California Capitol, Bursts into Flames."

[318] Malacarne, "Vehicle Tracking Geo-Fencing."

[319] Jeremy Straub, "On-Board Computers and Sensors Could Stop the next Car-Based Attack," The Conversation, November 2, 2017, http://theconversation.com/on-board-computers-and-sensors-could-stop-the-next-car-based-attack-86088.

[320] Jason Hanna, "TSA Warns Truckers: Watch for Possible Ramming Terror Attacks," CNN, May 5, 2017, https://www.cnn.com/2017/05/04/politics/tsa-ramming-terror-attacks-warning/index.html.

[321] Harre-Young, *The Relative Performance and Consequences*, 68.

[322] Noah J. Goodall, "From Trolleys to Risk: Models for Ethical Autonomous Driving," *American Journal of Public Health* 107, no. 4 (April 2017): 496–496, https://doi.org/10.2105/AJPH.2017.303672.

pedestrian actions.[323] With the merging of different information sources from databases and vehicle sensors, FAVs can be programmed simply not to have the ability to drive where they are not authorized and not harm others, and utilizing their connectivity, alert the proper authorities should attempts be made otherwise.

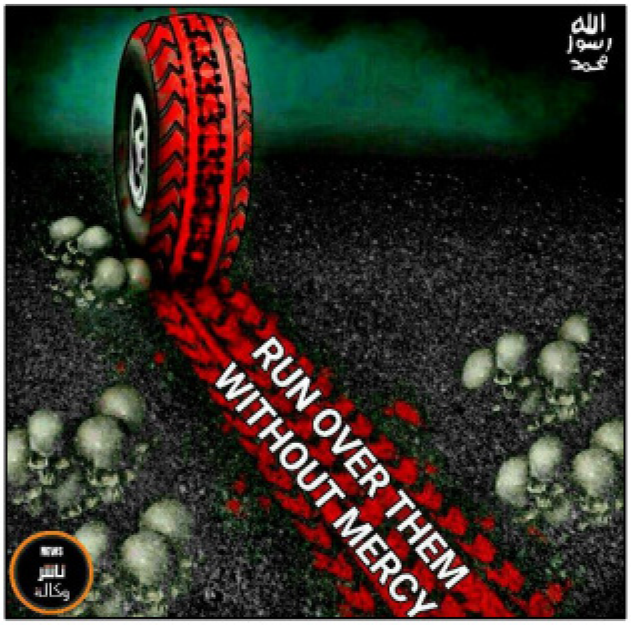


Figure 14. ISIS Propaganda Image from *Nashir* via pro-ISIS Telegram Channel, October 31, 2017[324]

2. FAVs Need the Ability to Identity Their Users

Whether it is for a call for a ride service where the vehicle is simply transporting a person to a location or delivering a package, the person using the FAV will need to be identified for preemptive analysis or should something actionable occur. For instance, if individuals were to summon a FAV to have a package delivered, they would be identified via the application on their phone or computer they used and also identified by the

[323] Zhijie Fang, David Vázquez, and Antonio M. López, “On-Board Detection of Pedestrian Intentions,” *Sensors (Basel, Switzerland)* 17, no. 10 (September 23, 2017): 2, https://doi.org/10.3390/s17102193.

[324] Source: Counter Extremism Project, *Vehicles as Weapons of Terror* (New York and London: Counter Extremism Project, Counter Extremism Project, 2019), 7.

vehicle itself through biometric methods via facial recognition, fingerprint, palm print, or voice identification to name a few.[325] User-authentication for the purposes of eliminating anonymity will be crucial for mitigating the threat of FAVBIEDs.

3. FAVs Need Internal Capabilities to Identity Intended or Unintended Cargo or Occupants

Should a FAV be used to deliver a package, it will be necessary to determine that a package is present within the designated cargo area of a vehicle, such as trunk, cabin, or frunk.[326] Once a package is delivered, the FAV needs to determine that it was actually removed by the intended recipient via biometric identification. In addition, the vehicle would need analytics for alerting about unintended uses. For instance, if a FAV is called to a business to receive a package that weighs approximately five pounds and the vehicle detects a weight change of 500 pounds or inconsistencies with the approximate size, there could be cause for concern and proper alerts would need to be made. Should occupants use a FAV, the vehicle would need to determine that everyone and everything vacated the vehicle upon arriving at the intended destination or the aforementioned Comic-Con scenario could happen again. Internal cameras, vehicle weight sensors, or combinations of other vehicle systems could help detect anomalies. New technologies are also being considered, such as the patent filed for autonomous vehicle unauthorized passenger or object detection.[327] Lastly, the identification component should be combined with other vehicle information that may be meaningful for incident follow-up and stored in the FAVs "black box" and even actively updated via connectivity to cloud storage or equivalent in real-time. Any FAV commercial application needs to implement payload interrogation at the outset of the system design process.

[325] John Chambers, "California Highway Patrol Golden Gate Division Supervisory Leadership Forum 2018" (forum, Castro Valley, California, October 2, 2018).

[326] "What Is a Frunk, and Why Does My Family Need One?," *Famlii* (blog), February 12, 2018, https://www.famlii.com/tesla-frunk-family-car-model-x/.

[327] Johannes Huennekens, Samuel Ellis, and Greg Foletta, Autonomous vehicle unauthorized passenger or object detection, United States US20170080900A1, filed September 18, 2015, and issued March 23, 2017, https://patents.google.com/patent/US20170080900A1/en.

4. FAVs Need Internal and External System Monitoring to Identify Unauthorized Computer System Access (aka Hacking), A Mechanism to Report Intrusions, and for the Vehicle to Have a Back-Up Safety Response Default Should Systems be Compromised

Cybersecurity will be critical for FAVs. Industry reports indicate 98% of new cars will be connected via cell networks by 2020 and constitute almost one-third of all cell devices.[328] Current non-autonomous vehicles are already susceptible to hacking. The connectivity with FAVs will only exponentially increase the threat. David Barzilai, co-founder of the Israeli cybersecurity company Karamba, states:

> Security bugs and vulnerabilities to hackers [increase] with direct relation to lines of code. A Boeing Dreamliner has 15 million lines. A contemporary premium car has 100 million. An autonomous car has more than 300 million.[329]

There is no choice. Connectivity with the IoT is a major vulnerability and it is imperative that FAV designs integrate strategies for continued adaptation to this evolving threat.[330] Once a cyber threat has been detected, notifications need to be made to vehicle occupants and the appropriate authorities. Lastly, a plan needs to be in place on how compromised vehicles will safely respond to a cyber intrusion depending on the severity of system penetration. Secure communications for FAVs will need to be a priority at the outset of the system design process.

5. FAVs Need the Ability to Receive and Act upon Instructions from External Inputs, such as Law Enforcement or Other Public Safety Agencies

In the event of a traffic advisory, the FAV needs the ability to receive information from the reporting agency, such as a state department of transportation, or an app, such as Waze, and adjust its route. Safety instruction is not just limited to vehicle systems involving interconnectivity. For instance, if a FAV comes upon slowed traffic resulting from a collision up ahead that is being diverted off the freeway by a state trooper via

[328] Berk, "We Hack a Car (It's Way Easier than You Might Think)."

[329] Berk.

[330] National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis, *Future Environmental Net Assessment*, 6.

hand signals, flashlight, cone patterns, flair patterns, or patrol vehicle directional lighting, the FAV should be able to interpret the instruction, exit the freeway appropriately, and adjust to a detoured route.

Additional law enforcement or public safety needs to include the ability for a FAV to respond appropriately to a forward facing red light and pull to the right to allow a patrol vehicle to pass or continue to pull to the right shoulder for an enforcement contact. A law enforcement override capability is also necessary for situations in which the occupant is at risk, such as a medical emergency, or when the occupant is a criminal being apprehended. FAVs may need to stop for cargo inspections or vehicle safety checks. First responder safety could be enhanced with personal body sensors detectable to FAVs that allow for stand-off distances. Special events, such as public gatherings, would need the ability for temporary geo-fencing or sensors to delineate which roadways are closed to FAVs. Instances also occur in which FAVs will need to be restricted for special circumstances, such as protective details or cycling races that require a moving safety perimeter secured by law enforcement until an event passes. Lastly, through connectivity, a need will also arise for remote monitoring of FAVs to help with the overall transportation network and the identification of specific vehicles by governmental agencies with the need to know and right to know. Overall, being a first responder is already a dangerous job, and it is essential to ensure FAVs do not cause additional difficulties and jeopardize their safety.

C. FUTURE RESEARCH

This discussion was not all-inclusive with regard to the topic of FAVBIEDs, as it was simply an attempt to contribute to the conversation regarding mitigating strategies as this topic becomes reality. Even with good intentions, the proposed mitigating strategies can have unintended consequences that will also be in need of deliberation.

Ethical concerns will be raised with regard to FAV integrated technologies constantly in communication with the IoT and personal privacy. With the identification of people utilizing FAVs, it is not unsurprising that different private industry and government databases will continually be accessed for the purpose of mitigating threats while also retaining data in the process. Vehicle manufacturers and technology companies currently associated with transportation products already retain volumes of data regarding the use of their goods and services.[331] Technology companies have also already demonstrated the ability to misuse this information.[332] Ultimately, will the population just have to accept industry and government access to information about people's daily lives as a part of the FAV interconnected experience?

This discussion was primarily constrained to passenger vehicles. Adding commercial vehicles to the FAVBIED topic compounds the mitigation imperative exponentially. A tractor-trailer combination is rated at an 80,000-pound gross vehicle weight capacity and already has a measurable difference in negative outcomes on the U.S. transportation network, such as an increased propensity for fatalities during traffic collisions.[333] A fully autonomous commercial vehicle (FACV) will be substantially more difficult to use safely in environments accessible to the general motoring public.[334] However, the cost savings with regard to their overall operation will be substantial; thus, the financial incentive will be a major force behind their development and mass deployment.[335] The deployment of FACVs will translate into increased availability for terrorists and thereby cause the need for enhancing FAVBIED mitigating strategies for this amplified threat.

Serious consideration needs to be given to how public safety officers will interact with FAV technology. Will law enforcement be empowered to override FAVs to restrict access to emergency incident locations or to fight crime? Constitutional arguments aside, could an officer simply have the ability to override a suspect vehicle remotely during a

[331] SAS Institute Inc., *The Connected Vehicle. Big Data, Big Opportunities* (Cary, NC: SAS Institute Inc., 2015), 5.

[332] Brad Stone, *The Upstarts: How Uber, Airbnb, and the Killer Companies of the New Silicon Valley Are Changing the World* (Boston, MA: Little, Brown and Company, 2017), 264.

[333] John Markoff, "In a Move to Self-Driving Cars, Big-Rig Trucks May Come First," *New York Times*, May 17, 2016, sec. B.

[334] David H. Freedman, "If Automation Is Already Messing with Our Economy and Our Politics, Just Wait until Self-Driving Trucks Arrive," *MIT Technology Review*, March/April 2017, https://www.technologyreview.com/s/603493/10-breakthrough-technologies-2017-self-driving-trucks/.

[335] Freedman.

high-speed chase or when possibly investigating an impaired driver who is manually driving the vehicle? Or, could a biometrically identified wanted felon using a FAV rideshare be remotely detoured to the local police department for apprehension?[336] Interestingly enough, new types of crime that have not even been imagined are not even taken into account as FAV technology becomes commonplace. Ultimately, law enforcement will absolutely want the ability to override and direct autonomous vehicles being used by terrorists or other criminals in the interests of public safety; but does the public agree?[337]

D. FINAL THOUGHTS

An open and forthright policy discussion with transparent expectations needs to be established at the federal regulatory level. The current free-for-all "hands off" policy by government oversight agencies is understandable given the strategic importance of winning the race to full autonomy. Yet, it is crucial to be fair and ask if this policy is contrary to public safety expectations. Does the general public really want to trust private industry with their safety without governmental checks and balances? The homeland security enterprise, specifically including the law enforcement community, needs to continue to be a part of the conversation with policy level decision making as it will be interacting with FAVs both figuratively and literally where the rubber meets the road. A bold new future where society is going to change radically with the advent of FAVs is on the horizon. Absent a security-based systems design approach, this nation will be reacting to, rather than preventing, the use of autonomous vehicles as explosives delivery systems. Now is the time for government and private industry leaders to engage, be forward thinking, and plan for the long-term success of FAVs and mitigate the threat of FAVBIEDs by working together toward this nation's overall national safety and security.

[336] Anouk Vleugels, "Police Can Remotely Drive Your Stolen Tesla into Custody," The Next Police|The Next Web, November 19, 2018, https://thenextweb.com/the-next-police/2018/11/19/police-control-your-self-driving-cars/?utm_campaign=OGshare.

[337] Martin C. Libicki, "The Police Could Be Controlling Your Self-Driving Car," April 2016, https://www.rand.org/blog/2016/04/the-police-could-be-controlling-your-self-driving-car.html.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Advocates for Highway and Auto Safety. “Statement of Jackie Gillan on DOT Release of Federal AV Policy.” *Advocates for Highway and Auto Safety* (blog), September 20, 2016. https://saferoads.org/2016/09/20/statement-of-jackie-gillan-on-dot-release-of-federal-av-policy/.

Alliance of Automobile Manufacturers. “Automotive Industry Collaborates in Developing Vehicle Cybersecurity Best Practices to Address Cybersecurity Challenges.” CISION PR Newswire, July 21, 2016. https://www.prnewswire.com/news-releases/automotive-industry-collaborates-in-developing-vehicle-cybersecurity-best-practices-to-address-cybersecurity-challenges-300301805.html.

Anderson, James M., Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, and Oluwatobi A. Oluwatola. *Autonomous Vehicle Technology: A Guide for Policymakers*. Santa Monica, CA: RAND, 2014.

Angel, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, and Brian Michael Jenkins et al. *The Lessons of Mumbai*. Santa Monica, CA: RAND, 2009.

Baker, David R. “How Self-Driving Cars Could Become Weapons of Terror.” *San Francisco Chronicle*. Updated October 11, 2016. http://www.sfchronicle.com/business/article/How-self-driving-cars-could-become-weapons-of-9958541.php.

Ball, Ryan Jokl. *The Proliferation of Unmanned Aerial Vehicles: Terrorist Use, Capability, and Strategic Implications*. Technical Report No. LLNL-TR-740336. Livermore, CA: Lawrence Livermore National Laboratory, 2017. https://doi.org/10.2172/1410035.

Barnes, Philip, and Eli Turkel. *Autonomous Vehicles in Delaware: Analyzing the Impact and Readiness for the First State*. Newark, DE: Institute for Public Administration, School of Public Policy and Administration, University of Delaware, 2017.

BBC News. “Venezuela President Maduro Survives ‘Drone Assassination Attempt.’” August 5, 2018. https://www.bbc.com/news/world-latin-america-45073385.

Berk, Brett. “We Hack a Car (It’s Way Easier than You Might Think).” *Automobile Magazine* (blog), January 11, 2019. https://www.automobilemag.com/news/car-hacking-we-hack-autonomous-car/?sc_cid=AppleNewsAMAGArticle.

Bigelow, Pete. "Auto Industry Unites to Take Countermeasures against Hackers." Car and Driver, June 10, 2016. https://blog.caranddriver.com/auto-industry-unites-to-take-countermeasures-against-hackers/.

Bloomberg, Michael R., Raymond W. Kelly, and Richard A. Falkenrath. "New York City Police Department, Engineering Security: Protective Design for High Risk Buildings." 105 (2009): 1–130.

Bonn, Scott A. "The Mass Shooting-Suicide Connection." *Psychology Today*, February 22, 2018. https://www.psychologytoday.com/blog/wicked-deeds/201802/the-mass-shooting-suicide-connection.

Bosher, Lee, and Andrew Dainty. "Disaster Risk Reduction and 'Built-in' Resilience: Towards Overarching Principles for Construction Practice." *Disasters* 35, no. 1 (2011): 1–18.

Bosher, Lee, Andrew Dainty, Patricia Carrillo, and Jacqueline Glass. "Built-in Resilience to Disasters: A Pre-emptive Approach." *Engineering, Construction and Architectural Management* 14, no. 5 (September 11, 2007): 434–46. https://doi.org/10.1108/09699980710780746.

Boudette, Neal E. "Big Carmakers Merge, Cautiously, Into Self-Driving Lane." *New York Times*, September 2, 2016.

Bunker, Robert J. "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices (AVBIEDs): Insurgent Use and Terrorism Potentials." TRENDS Research and Advisory, January 2016. http://trendsinstitution.org/daeshis-armored-vehicle-borne-improvised-explosive-devices-avbieds-insurgent-use-and-terrorism-potentials/.

Bunker, Robert J., and John P. Sullivan. *Cartel Car Bombings in Mexico*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

Casey, Michael. "Want a Self-Driving Car? Look on the Driveway." *Fortune*, December 6, 2014. http://fortune.com/2014/12/06/autonomous-vehicle-revolution/.

CBS Sacramento. "FROM THE ARCHIVE: Truck Intentionally Strikes California Capitol, Bursts into Flames." April 18, 2016. https://sacramento.cbslocal.com/2016/04/18/from-the-archive-truck-intentionally-strikes-california-capitol-bursts-into-flames/.

Center for Sustainable Systems. *Autonomous Vehicles Factsheets Mobility*. Ann Arbor, MI: University of Michigan, 2018. http://css.umich.edu/sites/default/files/Autonomous_Vehicles_Factsheet_CSS16-18_e2018_0.pdf.

CEPT Electronic Communications Committee. *Technical and Regulatory Aspects and the Needs for Spectrum Regulation for Unmanned Aircraft Systems (UAS)*. ECC Report 268. Copenhagen, Denmark: CEPT Electronic Communications Committee, 2017. https://www.cept.org/files/9522/Draft%20ECC%20Report%20268%20for%20PC.docx.

Chambers, John. "California Highway Patrol Golden Gate Division Supervisory Leadership Forum 2018." Forum, Castro Valley, California, October 2, 2018.

Chapple, James, and Agency staff. "Man Fined for Flying Drone over Parliament and Buck Palace." MyLondon, September 16, 2015. http://www.getwestlondon.co.uk/news/west-london-news/man-fined-flying-drone-over-10063456.

Cheney, Peter. "What's the Weakest Link in Your Car?." The Globe and Mail, July 31, 2013. https://www.theglobeandmail.com/globe-drive/culture/commuting/whats-the-weakest-link-in-a-car/article13499431/.

Cherry, Christopher, Anastasia Loukaitou-Sideris, and Martin Wachs. "Subway Station Design and Management: Lessons from Case Studies of Contemporary Terrorist Incidents." *Journal of Architectural and Planning Research* 25, no. 1 (Spring 2008): 76–90.

Clamann, Michael, Miles Aubert, and Mary L. Cummings. *Evaluation of Vehicle-to-Pedestrian Communication Displays for Autonomous Vehicles*. Berlin, Germany: ResearchGate, 2017.

Clerkin, Bridget. "How Will We Ensure Security in a Self-Driving World?." DMV, September 21, 2017. https://www.dmv.org/articles/cybersecurity-and-self-driving-cars.

CNN. "Judges Targeted Fast Facts." Updated April 18, 2018. https://www.cnn.com/2013/11/04/us/judges-targeted-fast-facts/index.html.

Condliffe, Jamie. "Can a Chinese Drone Manufacturer's No-Fly Zone Software Stop ISIS from Weaponizing Drones?." *MIT Technology Review*, April 26, 2017. https://www.technologyreview.com/s/604279/can-djis-no-fly-zone-software-stop-isis-from-weaponizing-drones/.

Condon, Tim. "Leading the Way to AV Safety." *VIA Magazine*, 2019.

Conn, David. "Dortmund Attack: How Soccer Has Became a Target of Terrorists." *The Irish Times*, April 12, 2017. https://www.irishtimes.com/sport/soccer/champions-league/dortmund-attack-how-soccer-has-became-a-target-of-terrorists-1.3046763.

Conroy, Pat, Anupam Narula, Frank Milano, and Raj Singhal. "Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry." Deloitte Insights, November 13, 2014. https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html.

Cooper, Brent R. "Event Data Recorders: Balancing the Benefits and Drawbacks." IRMI, August 2008. https://www.irmi.com/articles/expert-commentary/event-data-recorders-balancing-the-benefits-and-drawbacks.

Cornell Law School, Legal Information Institute. "15 CFR 730.3—'Dual Use' and Other Types of Items Subject to the EAR." Accessed January 28, 2019. https://www.law.cornell.edu/cfr/text/15/730.3.

Counter Extremism Project. *Vehicles as Weapons of Terror*. New York and London: Counter Extremism Project, Counter Extremism Project, 2019.

Da-Jiang Innovations. *DJI Remote Identification Whitepaper*. Nanshan District, Shenzhen, China: Da-Jiang Innovations, 2017. https://www.dropbox.com/s/v4lkyr2kdp8ukvx/DJI%20Remote%20Identification%20Whitepaper%203-22-17.pdf?dl=0.

Davis, Mike. "Car Bombs with Wings: A History of the Car Bomb (Part 2)." TomDispatch, April 13, 2006. http://www.tomdispatch.com/post/76824/.

———. "Poor Man's Air Force, A History of the Car Bomb." *Coldtype.Net*, 2006.

Department of Homeland Security. *Potential Threat to Homeland Using Heavy Transport Vehicles*. Washington, DC: Department of Homeland Security, 2004.

Department of Transportation. *AV Fact Sheet—Model State Policy*. Washington, DC: Department of Transportation, 2016. https://www.transportation.gov/AV/av-fact-sheet-model-state-policy.

———. *AV Fact Sheet—Vehicle Performance Guidance*. Washington, DC: Department of Transportation, 2016. https://www.transportation.gov/AV/av-fact-sheet-vehicle-performance-guidance.

Deputy Chief of Staff for Intelligence, Assistant Deputy Chief of Staff for Intelligence—Threats. *Suicide Bombing in the COE*. Fort Eustis, VA: U.S. Army Training and Doctrine Command, 2005.

Dhanya Nair, Shweta Desai, Swapnil Rawal, Shashank Shekhar, Sukanya Shetty, Prashant Rangnekar, and Smita Nair et al. "Tracing the Terror Route." The Indian Express, Journalism of Courage Archive, December 10, 2008. http://archive.indianexpress.com/news/tracing-the-terror-route/396335/1.

DJI Official. “DJI Introduces New Geofencing System for Its Drones.” Accessed June 26, 2018. https://www.dji.com/newsroom/news/dji-fly-safe-system.

Dubno, Daniel, Dr. Stephen Flynn, Dr. Yacov Haimes, and Byron Collie. “Autonomous Technology White Paper, Homeland Security Science and Technology Advisory Committee (HSSTAC) Quadrennial Homeland Security Review Subcommittee.” *Homeland Security, Science and Technology*, March 10, 2017.

ECRRN European Cyber Resilience Research Network. “6 Steps Risk Management Approach.” *ECRRN European Cyber Resilience Research Network* (blog), March 9, 2016. https://www.ecrrn.com/blog/files/6b05d547c39af8ce6babd9e94b71fab0-4.html.

Famlii. “What Is a Frunk, and Why Does My Family Need One?.” *Famlii* (blog), February 12, 2018. https://www.famlii.com/tesla-frunk-family-car-model-x/.

Fang, Zhijie, David Vázquez, and Antonio M. López. “On-Board Detection of Pedestrian Intentions.” *Sensors (Basel, Switzerland)* 17, no. 10 (September 23, 2017): 1–14. https://doi.org/10.3390/s17102193.

Farnam Street. “Complexity Bias: Why We Prefer Complicated to Simple.” *Farnam Street* (blog), January 8, 2018. https://fs.blog/2018/01/complexity-bias/.

———. “Inversion: The Power of Avoiding Stupidity.” *Farnam Street* (blog), October 28, 2013. https://fs.blog/2013/10/inversion/.

———. “Mental Models: The Best Way to Make Intelligent Decisions (109 Models Explained).” *Farnam Street* (blog), accessed January 13, 2019. https://fs.blog/mental-models/.

Federal Aviation Administration, Department of Transportation. “Aeronautics and Space: Part 1—Definitions and Abbreviations.” *Electronic Code of Federal Regulations*, title 14 (1962). https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=a3a21673a5020d6763cfb10d068366d8&rgn=div5&view=text&node=14:1.0.1.1.1&idno=14#14:1.0.1.1.1.0.1.1.

Federal Bureau of Investigation. “Motor Vehicles Increasingly Vulnerable to Remote Exploits.” March 17, 2016. https://www.ic3.gov/media/2016/160317.aspx.

Fedorschak, Kevin C., and Kena Fedorschak. “Autonomous Vehicles Will Have Tremendous Impacts on Government Revenue.” *Brookings* (blog), July 7, 2015. https://www.brookings.edu/blog/techtank/2015/07/07/autonomous-vehicles-will-have-tremendous-impacts-on-government-revenue/.

Fraade-Blanar, Laura, and Nidhi Kalra. *Autonomous Vehicles and Federal Safety Standards: An Exemption to the Rule?* Santa Monica, CA: RAND, 2017.

Freedman, David H. “If Automation Is Already Messing with Our Economy and Our Politics, Just Wait until Self-Driving Trucks Arrive.” *MIT Technology Review*, March/April 2017. https://www.technologyreview.com/s/603493/10-breakthrough-technologies-2017-self-driving-trucks/.

Garsten, Ed. “Sharp Growth in Autonomous Car Market Value Predicted but May Be Stalled by Rise in Consumer Fear.” *Forbes*, August 13, 2018. https://www.forbes.com/sites/edgarsten/2018/08/13/sharp-growth-in-autonomous-car-market-value-predicted-but-may-be-stalled-by-rise-in-consumer-fear/.

Gibbs, Phil, and Sugihara Hiroshi. “What Is Occam’s Razor?.” University of California, Riverside, Department of Mathematics, 1997. http://math.ucr.edu/home/baez/physics/General/occam.html.

Gibson, Jake. “Timeline of Recent Vehicle Attacks in U.S., Europe.” Fox News, November 1, 2017. http://www.foxnews.com/world/2017/11/01/timeline-recent-vehicle-attacks-in-us-europe.html.

Goodall, Noah J. “From Trolleys to Risk: Models for Ethical Autonomous Driving.” *American Journal of Public Health* 107, no. 4 (April 2017): 496–496. https://doi.org/10.2105/AJPH.2017.303672.

Goodman, Marc. “How Terrorists Are Turning Robots into Weapons.” Defense One, April 16, 2015. http://www.defenseone.com/ideas/2015/04/how-terrorists-are-turning-robots-weapons/110362/.

Government Accountability Office. *Long-range Emerging Threats Facing the United States As Identified by Federal Agencies*. GAO-19-204SP. Washington, DC: Government Accountability Office, 2018.

———. *Report to Congressional Committees, Internet of Things, Enhanced Assessments and Guidance Are Needed to Address Security Risks in DoD*. GAO-17-668. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/assets/690/686203.pdf.

Grabowski, Martha, John Harrald, Rene Van Dorp, Thomas Mazzuchi, Irmak Renda Tanali, Sunil Shrestha, and Noraida Abdul Ghani et al. *The Washington State Ferries Risk Assessment Final Report*. Washington, DC: The George Washington University; Troy, NY: Rensselaer Polytechnic Institute; Richmond, VA: Virginia Commonwealth University, 1999.

Graham, Gordon. *Affairs of Government 2016: Some Thoughts on Real Risk Management*. Orem, UT: Utah Risk Management Mutual Association, 2016. https://www.urmma.org/wp-content/uploads/2016/03/Gordon-Graham-2016-Handout.pdf.

Greenberg, Andy. “A New Wireless Hack Can Unlock 100 Million Volkswagens.” WIRED, July 10, 2016. https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/.

———. “Hackers Cut a Corvette’s Brakes via a Common Car Gadget.” WIRED, August 11, 2015. https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/.

———. “Securing Driverless Cars from Hackers Is Hard. Ask the Ex-Uber Guy Who Protects Them.” WIRED, April 12, 2017. https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.

———. “Tesla Responds to Chinese Hack with a Major Security Upgrade.” WIRED, September 27, 2016. https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/.

———. “The FBI Warns That Car Hacking Is a Real Risk.” WIRED, March 17, 2016. https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/.

Griggs, Mary Beth. “The FBI’s Next Worry: Self-Driving Car Bombs.” *Smithsonian*, July 17, 2014. https://www.smithsonianmag.com/smart-news/fbi-worried-self-driving-cars-could-be-used-bombs-180952082/.

Grossman, Dave. “Are Video Games Breeding an Assassination Generation?.” Daily Beast, November 18, 2016. https://www.thedailybeast.com/articles/2016/11/18/are-video-games-breeding-an-assassination-generation.

Hamm, Mark, and Ramon Spaaj. *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*. Terre Haute, IN: Indiana State University, 2015.

Hammes, Thomas X. *The Sling and the Stone: On War in the 21st Century*. St. Paul, MN: Zenith Press, 2006.

Hanna, Jason. “TSA Warns Truckers: Watch for Possible Ramming Terror Attacks.” CNN, May 5, 2017. https://www.cnn.com/2017/05/04/politics/tsa-ramming-terror-attacks-warning/index.html.

Harre-Young, Steven Nicholas. *The Relative Performance and Consequences of Protecting Crowded Places from Vehicle-Borne Improvised Explosive Device*. Loughborough, UK: Loughborough University, 2012. https://dspace.lboro.ac.uk/2134/9757.

Harris, Mark. “FBI Warns Driverless Cars Could Be Used as ‘Lethal Weapons.’” *The Guardian*, July 16, 2014. http://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous.

Hays, Tom. "AP Was There: The 1993 Bombing of the World Trade Center." AP News, February 26, 2018. https://apnews.com/f4f1fd2b2d4b4a17b94ca7183fb65ba4.

Herberger, Carl. "Why the Department of Transportation's Self-Driving Car Guidelines Aren't Enough." *TechCrunch* (blog), November 6, 2016. http://social.techcrunch.com/2016/11/06/why-the-department-of-transportations-self-driving-car-guidelines-arent-enough/.

Hill, Simon. "Android vs. IOS: In-Depth Comparison of the Best Smartphone Platforms." Digital Trends, January 17, 2019. https://www.digitaltrends.com/mobile/android-vs-ios/.

Huennekens, Johannes, Samuel Ellis, and Greg Foletta. Autonomous vehicle unauthorized passenger or object detection, United States US20170080900A1, filed September 18, 2015, and issued March 23, 2017. https://patents.google.com/patent/US20170080900A1/en.

India Today. "How 26/11 Mumbai Attack Happened in 2008: From First Eyewitness to Kasab." November 26, 2017. https://www.indiatoday.in/india/story/how-2611-mumbai-terror-attack-happened-in-2008-from-first-eyewitness-to-kasab-1094473-2017-11-26.

Intel. "Car of the Future, Trends in Next-Generation Automotive Safety and Security." *Intel* 1 (Winter 2017): 2–10.

IoT Agenda. "What Is Car Hacking?." Accessed November 5, 2017. http://internetofthingsagenda.techtarget.com/definition/car-hacking.

Jackson, Brian A., David R. Frelinger, Michael J. Lostumbo, and Robert W. Buttons. *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles*. Santa Monica, CA: RAND National Defense Research Institute, 2008.

Jacobo, Julia. "A Look Back at the Aurora, Colorado, Movie Theater Shooting 5 Years Later." ABC News, July 20, 2017. https://abcnews.go.com/US/back-aurora-colorado-movie-theater-shooting-years/story?id=48730066.

Jenkins, Brian Michael. "Brian Jenkins: Terrorists Can Use Cars, Trucks and Vans to Kill Their Targets. What's the Best Way to Keep People Safe?." Fox News, last updated September 19, 2017. http://www.foxnews.com/opinion/2017/09/03/brian-jenkins-terrorists-can-use-cars-trucks-and-vans-to-kill-their-targets-whats-best-way-to-keep-people-safe.html.

Jenkins, Brian Michael, and Bruce R. Butterworth. *Terrorist Vehicle Attacks on Public Surface Transportation Targets*. San Jose, CA: Mineta Transportation Institute, San Jose State University, 2017. http://transweb.sjsu.edu/sites/default/files/terrorist-vehicle-attacks-on-public-surface-transportation-targets_0.pdf.

Jensen, Bart. “Small Drone Crashes near White House despite Ban against Flights in D.C.” USA TODAY, October 9, 2015. https://www.usatoday.com/story/news/2015/10/09/drone-crash-white-house-ellipse-us-park-police-federal-aviation-administration/73641812/.

Jofre, Shelley. “The Batman Killer—A Prescription for Murder?.” BBC News, July 26, 2017. https://www.bbc.co.uk/news/resources/idt-sh/aurora_shooting.

Joint Counterterrorism Assessment Team. *VBIED-Preparedness-Recognition-Response-ONLINE-Version*. Washington, DC: Office of the Director of National Intelligence, 2018. https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/VBIED-Preparedness-Recognition-Response-ONLINE-Version.pdf.

Jones, Susan. “‘Autonomous Vehicles Provide an Avenue for Terrorism,’ Congress Is Told.” CNSNews, February 15, 2017. https://www.cnsnews.com/news/article/susan-jones/autonomous-vehicles-provide-avenue-terrorism-congress-told.

Kaaman, Hugo. “The Evolution of Suicide Car Bombs Examined.” Action on Armed Violence, August 23, 2017. https://aoav.org.uk/2017/evolution-suicide-car-bombs/.

Kalra, Nidhi, and Susan M. Paddock. “Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?.” *Transportation Research Part A: Policy and Practice* 94 (2016): 1–15.

Kaplan, Robert S., and Anette Mikes. “Managing Risks: A New Framework.” *Harvard Business Review*, June 1, 2012. https://hbr.org/2012/06/managing-risks-a-new-framework.

Kapusta, Philip E. “Suicide Bombers in CONUS.” Monograph, School of Advanced Military Studies United States Army Command and General Staff College, 2007.

Karsten, Müller, and Carlo Schwarz. “Fanning the Flames of Hate: Social Media and Hate Crime.” *SSRN Electronic Journal* 373 (May 2017): 1–35. https://doi.org/10.2139/ssrn.3082972.

Kean, Thomas H., and Lee Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks, 2004.

Kelley, Ben. “Miles to Go on Highway Safety.” *FairWarning.Org* (blog), September 7, 2016. https://www.fairwarning.org/2016/09/miles-go-highway-safety/.

Knight, Will. “GM’s CEO, Mary Barra, Says the Threat of Cars Being Hacked Will Pose a Risk to the Entire Car Industry.” *MIT Technology Review*, July 22, 2016. https://www.technologyreview.com/s/601957/gm-ceo-car-hacking-will-become-a-public-safety-issue/.

Kraul, Chris, and Mery Mogollon. “Venezuela Says Assassination Attempt Used Drones Loaded with 2 Pounds of Plastic Explosives.” *Los Angeles Times*, August 5, 2018. http://www.latimes.com/world/la-fg-venezuela-drone-attack-20180805-story.html.

Latham, Ann. “What The Heck Is A Strategy Anyway?.” *Forbes*, October 29, 2017. https://www.forbes.com/sites/annlatham/2017/10/29/what-the-heck-is-a-strategy-anyway/.

Lee, Jane J. “7 Other Sports-Related Attacks.” National Geographic News, April 16, 2013. https://news.nationalgeographic.com/news/2013/03/130415-sports-marathon-olympics-bombers-culture/.

Lewis, Jeffrey W. “A Smart Bomb in Every Garage? Driverless Cars and the Future of Terrorist Attacks.” National Consortium for the Study of Terrorism and Responses to Terrorism, September 28, 2015. http://www.start.umd.edu/news/smart-bomb-every-garage-driverless-cars-and-future-terrorist-attacks.

Lewis, Jeffrey William. “The Human Use of Human Beings: Suicide Bombing, Technological Innovation, and the Asymmetry of Modern Warfare.” *Global Politics Review* 2, no. 2 (October 2016): 9–27.

Lewis, Paul, Gregory Rogers, and Stanford Turner. *Beyond Speculation Automated Vehicles and Public Policy—An Action Plan for Federal, State, and Local Policymakers*. Washington, DC: Eno Center for Transportation, 2017. https://www.enotrans.org/wp-content/uploads/2017/04/AV_FINAL-1.pdf?x43122.

Libicki, Martin C. “The Police Could Be Controlling Your Self-Driving Car.” April 2016. https://www.rand.org/blog/2016/04/the-police-could-be-controlling-your-self-driving-car.html.

Lienert, Paul, and Joseph White. “Automakers, Google Take Different Roads to Automated Cars.” *Reuters*, September 4, 2015. https://www.reuters.com/article/us-autos-selfdriving-gurus-insight-idUSKCN0R40BX20150904.

Litman, Todd. *Autonomous Vehicle Implementation Predictions Implications for Transport Planning*. Victoria, BC, Canada: Victoria Transport Policy Institute, 2017. http://leempo.com/wp-content/uploads/2017/03/M09.pdf.

Locke, Cathy. “Ask Sacto 911 Crime Q&A: What Happened to Man Who Crashed Semi Truck into State Capitol in 2001?.” *Sacramento Bee*, January 2016. https://www.sacbee.com/news/local/crime/article53249580.html.

Logan, Bryan. "Police Stopped a Tesla Operating on Autopilot with Drunk Driver Asleep." *Business Insider*, December 1, 2018. https://www.businessinsider.com/police-stopped-an-autopilot-driven-tesla-with-drunk-driver-asleep-2018-11.

Mach, Ernst. *On Thought Experiments*. Translated by W. O. Price and Sheldon Krimsky. Medford, MA: Tufts University, 1972. https://sites.tufts.edu/sheldonkrimsky/files/2018/05/pub1973OnThoughtExperiments.pdf.

Majumder, Soumyajit. "26/11 Mumbai Attacks Anniversary: A War Waged against India." NDTV, November 25, 2017. https://www.ndtv.com/mumbai-news/26-11-mumbai-attacks-anniversary-a-war-waged-against-india-1779783.

Malacarne, Eleonora. "Vehicle Tracking Geo-Fencing: UK Exploring Technology against Terrorism." Transpoco, August 10, 2017. https://www.transpoco.com/blog/vehicle-tracking-geo-fencing-uk-exploring-technology-against-terrorism.

Marcou, Dan. "Armed in America: It's Not Easy Being a Retired Cop." PoliceOne, November 14, 2018. https://www.policeone.com/gun-legislation-law-enforcement/articles/482065006-Armed-in-America-Its-not-easy-being-a-retired-cop/.

Markoff, John. "In a Move to Self-Driving Cars, Big-Rig Trucks May Come First." *New York Times*, May 17, 2016.

Massimilia, Jeffrey. "Connected, Self-Driving Cars Pose Serious New Security Challenges." IndustryWeek, July 25, 2016. http://www.industryweek.com/emerging-technologies/connected-self-driving-cars-pose-serious-new-security-challenges.

Masunaga, Samantha. "Venezuela Attack Shows Drones Can Become Assassins. Here's How They Can Be Grounded." *Los Angeles Times*, August 6, 2018. http://www.latimes.com/business/la-fi-venezuela-counterdrone-20180806-story.html.

Mathis, Terry. "Low Probability Risks Can't Be Ignored." The Compass, ASSE Management Practice Specialty Newsletter, June 2003.

May, Patrick. "Firefighters Decry Drone Interference—One Pilot Arrested." *Mercury News*, October 16, 2017. https://www.mercurynews.com/2017/10/16/firefighters-say-drones-interfered-with-their-work-one-pilot-arrested/.

McFadden, Clark, and Dewey Ballantine. *International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings; Session 6—Dual-Use Technologies and National Security*. Washington, DC: The National Academies Press, 1997. https://doi.org/10.17226/5902.

McLeod, Saul. "Social Identity Theory." SimplyPsychology, 2008. https://www.simplypsychology.org/social-identity-theory.html.

Military.com. “ISIS Releases Photos of Militants Using U.S. M113s as VBIEDS.” October 30, 2014. https://www.military.com/defensetech/2014/10/30/isis-releases-photos-of-militants-using-u-s-m113s-as-vbieds.

Mortimer, Gary. “UAvionix Release Remote Identification White Paper.” *SUAS News—The Business of Drones* (blog), April 4, 2017. https://www.suasnews.com/2017/04/uavionix-release-remote-identification-white-paper/.

National Conference of State Legislatures. “Autonomous Vehicles|Self-Driving Vehicles Enacted Legislation.” November 7, 2018. http://www.ncsl.org/research/transporttation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#Enacted%20Autonomous%20Vehicle%20Legislation.

National Highway Traffic Safety Administration. *Cybersecurity Best Practices for Modern Vehicles*. Washington, DC: National Highway Traffic Safety Administration, 2016. https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

National Highway Transportation Safety Agency. *Federal Automated Vehicles Policy—Accelerating the Next Revolution in Roadway Safety*. Washington, DC: Department of Transportation, 2016. https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.

———. “Guidance Covers Cybersecurity Best Practices for All Motor Vehicles, Individuals and Organizations Manufacturing and Designing Vehicle Systems and Software.” October 24, 2016. https://www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle.

National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis. *Future Environmental Net Assessment: Autonomous Vehicles*. Washington, DC: Department of Homeland Security, 2017.

National Safety Council. *NSC Motor Vehicle Fatality Estimates*. Itasca, IL: National Safety Council, 2017. https://www.nsc.org/portals/0/documents/newsdocuments/2018/december_2017.pdf.

New York Times, Amanda Taub, and Max Fisher. “Facebook Fueled Anti-Refugee Attacks in Germany, New Research Suggests.” August 23, 2018. https://www.nytimes.com/2018/08/21/world/europe/facebook-refugee-attacks-germany.html.

Nol, David, and Barbara Peterson. “12 Plane Crashes that Changed Aviation.” *Popular Mechanics*, August 4, 2017. https://www.popularmechanics.com/technology/aviation/crashes/10-airplane-crashes-that-changed-aviation.

Novak, Matt. “The National Automated Highway System that Almost Was.” *Smithsonian*, May 16, 2013. https://www.smithsonianmag.com/history/the-national-automated-highway-system-that-almost-was-63027245/.

Office of the Director of National Intelligence. "JCAT Counterterrorism Guide for Public Safety Personnel." Accessed January 13, 2019. https://www.dni.gov/nctc/jcat/index.html.

Paez, Danny. "Tesla's Software-First Approach Foreshadows the Future of Cars." Inverse, December 2, 2018. https://www.inverse.com/article/51390-tesla-electric-cars-software.

Parrott, Roxanne. "How Does Anderson Cooper's Statement, 'Hope Is Not a Plan' Fit Today's Events?." *Talking about Health; Why Health Communication Matters* (blog), August 8, 2011. http://whyhealthcommunication.com/whc_blog/2011/08/08/how-does-anderson-coopers-statement-hope-is-not-a-plan-fit-todays-events/.

Paul, Kari. "Apple or Android? Here Is the Most Secure Phone You Can Get." MarketWatch, January 6, 2019. https://www.marketwatch.com/story/apple-or-android-here-is-the-most-secure-phone-you-can-get-2018-10-10.

Peterson, Barbara. "How Airport Security Has Changed Since 9/11." *Condé Nast Traveler*, September 10, 2016. https://www.cntraveler.com/story/how-airport-security-has-changed-since-september-11.

Petit, Frederic, Gilbert W. Bassett, W. A. Buehring, M. J. Collins, D. C. Dickinson, R. A. Haffenden, and A. A. Huttenga et al. *Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability*. Lemont, IL: Argonne National Laboratory, 2013.

Poulin, Chris. "Connected Car Security: Separating Fear from Fact." *TechCrunch* (blog), October 23, 2015. http://social.techcrunch.com/2015/10/23/connected-car-security-separating-fear-from-fact/.

Poulsen, Kevin. "Why the U.S. Government Is Terrified of Hobbyist Drones." *WIRED*, February 5, 2015. https://www.wired.com/2015/02/white-house-drone/.

Project, Counter Extremism. *Terror Targets in the West: Where and Why*. New York and London: Counter Extremism Project, n.d. Accessed January 21, 2019. https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/CEP_Terror_Targets.pdf.

Prokupecz, Shimon. Eric Levenson, Brynn Gingras, and Steve Almasy. "ISIS Note Found near Truck Used in Manhattan Terror Attack." CNN, November 6, 2017. http://www.cnn.com/2017/10/31/us/new-york-shots-fired/index.html.

Prusak, Larry. "What Can't Be Measured." *Harvard Business Review*, October 7, 2010. https://hbr.org/2010/10/what-cant-be-measured.

Ramsay, Stuart. “Exclusive: Inside IS Terror Weapons Lab.” Sky News, January 5, 2016. https://news.sky.com/story/exclusive-inside-is-terror-weapons-lab-10333883.

Randall, Tom. “Tesla’s Autopilot Vindicated with 40% Drop in Crashes.” *Bloomberg*, January 19, 2017. https://www.bloomberg.com/news/articles/2017-01-19/tesla-s-autopilot-vindicated-with-40-percent-drop-in-crashes.

Rassler, Don. *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*. Lincoln Hall, West Point, NY: Combating Terrorism Center at West Point United States Military Academy, 2016.

Riedman, David. “Incidents by Injured and Killed Annually.” *K-12 School Shooting Database* (blog), August 25, 2018. https://www.chds.us/ssdb/incidents-by-injured-killed-annually/.

Ross, Michaela. “Thune, Peters Eye Self-Driving Car Bill.” Bloomberg Law, BNA, February 15, 2017. https://www.bna.com/thune-peters-eye-n57982083844/.

Saltzman, Aaron. “As Risky as It Sounds, a Hands-off Approach to Driverless Vehicle Safety May Save Lives.” CBC News, September 15, 2017. http://www.cbc.ca/news/business/autonomous-vehicles-self-driving-cars-uber-google-general-motors-1.4287591.

SAS Institute Inc. *The Connected Vehicle. Big Data, Big Opportunities*. Cary, NC: SAS Institute Inc., 2015.

Silver, Andrew. “Autonomous Technology May Encourage a False Sense of Security.” Trucker, September 10, 2017. http://trucker.com/technology/autonomous-technology-may-encourage-false-sense-security.

Singer, Peter W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Press, 2009.

Slovick, Murray. “Security Issues Could Still Crimp the Self-Driving Car.” Electronic Design, June 28, 2017. http://www.electronicdesign.com/automotive/security-issues-could-still-crimp-self-driving-car.

Sneed, Annie. “The Most Vulnerable Ransomware Targets Are the Institutions We Rely on Most.” *Scientific American*, March 23, 2016. https://www.scientificamerican.com/article/the-most-vulnerable-ransomware-targets-are-the-institutions-we-rely-on-most/.

Stone, Brad. *The Upstarts: How Uber, Airbnb, and the Killer Companies of the New Silicon Valley Are Changing the World*. Boston, MA: Little, Brown and Company, 2017.

Straub, Jeremy. “On-Board Computers and Sensors Could Stop the next Car-Based Attack.” The Conversation, November 2, 2017. http://theconversation.com/on-board-computers-and-sensors-could-stop-the-next-car-based-attack-86088.

Subcommittee on Domestic Improvised Explosive Devices. *Research Challenges in Combating Terrorist Use of Explosives in the United States*. Washington, DC: National Science and Technology Council, 2008.

Temple, James. “Evidence Is Piling up That Facebook Can Incite Violence.” *MIT Technology Review*, August 21, 2018. https://www.technologyreview.com/the-download/611920/evidence-is-piling-up-that-facebook-can-incite-racial-violence/.

Threlfall, Richard. *Autonomous Vehicles Readiness Index*. Amstelveen, Netherlands: KPMG International, 2018.

Tremlett, Giles, and Michael Walker. “Football Fans Flee Madrid Blast.” *Guardian*, May 2, 2002. https://www.theguardian.com/world/2002/may/02/football.spain.

TRIPwire. *DHS-DOJ Bomb Threat Stand-off Card*. Washington, DC: Department of Homeland Security, n.d. Accessed January 21, 2019. https://tripwire.dhs.gov/IED/resources/docs/DHS-DOJ%20Bomb%20Threat%20Stand-off%20Card.pdf.

Turak, Natasha. “More than 100 Politicians Murdered in Mexico Ahead of Election.” CNBC, June 26, 2018. https://www.cnbc.com/2018/06/26/more-than-100-politicians-murdered-in-mexico-ahead-of-election.html.

Uranga, Rachel. “Port of L.A.’s Automated Terminal: Future of Commerce or Blue-Collar Job-Killer?.” *Press Telegram* (blog), March 18, 2017. http://www.presstelegram.com/business/20170318/port-of-las-automated-terminal-future-of-commerce-or-blue-collar-job-killer.

US-CERT United States Computer Emergency Readiness Team. “Ransomware.” Accessed January 22, 2019. https://www.us-cert.gov/Ransomware.

Valdovinos, Maria, James Specht, and Jennifer Zeunik. *Community Policing & Unmanned Aircraft Systems (UAS) Guidelines to Enhance Community Trust*. Washington, DC: Office of Community Oriented Policing Services, 2016.

van der Bruggen, Koos. “Possibilities, Intentions and Threats: Dual Use in the Life Sciences Reconsidered.” *Science and Engineering Ethics* 18, no. 4 (December 2012): 741–56. https://doi.org/10.1007/s11948-011-9266-2.

Vleugels, Anouk. “Police Can Remotely Drive Your Stolen Tesla into Custody.” The Next Police|The Next Web, November 19, 2018. https://thenextweb.com/the-next-police/2018/11/19/police-control-your-self-driving-cars/?utm_campaign=OGshare.

Volz, Dustin. “Justice Dept. Group Studying National Security Threats of Internet-Linked Devices.” *Reuters*, September 9, 2016. https://www.reuters.com/article/us-usa-cyber-justice/justice-dept-group-studying-national-security-threats-of-internet-linked-devices-idUSKCN11F2FP.

Yoder, Jean. “Vehicle-to-Vehicle Communication.” National Highway Transportation Safety Agency, October 26, 2016. https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication.

Zur, Itamar. “Make No Mistake: Amazon Is Going to Take on Delivery Behemoths FedEx and UPS.” *Medium* (blog), May 17, 2018. https://medium.com/@itamarzur/make-no-mistake-amazon-is-going-to-take-on-delivery-behemoths-fedex-and-ups-d047cf6b6b0c.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California