SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Transportation, Terrorism and Crime: Deterrence, Disruption and Resilience

Daniel C. Goodrich, MPA
Frances L. Edwards, PhD

MINETA TRANSPORTATION INSTITUTE

LEAD UNIVERSITY OF

Mineta Consortium for Transportation Mobility

Founded in 1991, the Mineta Transportation Institute (MTI), an organized research and training unit in partnership with the Lucas College and Graduate School of Business at San José State University (SJSU), increases mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development, and technology transfer, we help create a connected world. MTI leads the four-university Mineta Consortium for Transportation Mobility, a Tier 1 University Transportation Center funded by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology (OST-R), the California Department of Transportation (Caltrans), and by private grants and donations.

MTI's transportation policy work is centered on three primary responsibilities:

Research

MTI works to provide policy-oriented research for all levels of government and the p rivate sector to foster the development of optimum surface transportation systems. Research areas include: bicycle and pedestrian issues; financing public and private sector transportation improvements; intermodal connectivity and integration; safety and security of transportation systems; sustainability of transportation systems; transportation / land use / environment; and transportation planning and policy development. Certified Research Associates conduct the research. Certification requires an advanced degree, generally a Ph.D., a record of academic publications, and professional references. Research projects culminate in a peer-reviewed publication, available on TransWeb, the MTI website (http://transweb.sjsu.edu).

Education

The Institute supports education programs for students seeking a career in the development and operation of surface transportation systems. MTI, through San José State University, offers an AACSB-accredited Master of Science in Transportation Management and graduate certificates in Transportation Management, Transportation Security, and High-Speed Rail Management that serve to prepare the nation's transportation managers for the 21st century. With the active assistance of the California Department of Transportation (Caltrans), MTI delivers its classes over a state-of-the-art videoconference network throughout the state of California and via webcasting beyond, allowing working transportation professionals to pursue an advanced degree regardless of their location. To meet the needs of employers seeking a diverse workforce, MTI's education program promotes enrollment to under-represented groups.

Information and Technology Transfer

MTI utilizes a diverse array of dissemination methods and media to ensure research results reach those responsible for managing change. These methods include publication, seminars, workshops, websites, social media, webinars, and other technology transfer mechanisms. Additionally, MTI promotes the availability of completed research to professional organizations and journals and works to integrate the research findings into the graduate education program. MTI's extensive collection of transportation- related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the information presented herein. This document is disseminated in the interest of information exchange. The report is funded, partially or entirely, by a grant from the U.S. Department of Transportation's University Transportation Centers Program. This report does not necessarily reflect the official views or policies of the U.S. government, State of California, or the Mineta Transportation Institute, who assume no liability for the contents or use thereof. This report does not constitute a standard specification, design standard, or regulation.

REPORT 19-36

TRANSPORTATION, TERRORISM AND CRIME: DETERRENCE, DISRUPTION AND RESILIENCE

Daniel C. Goodrich, MPA, CEM, MEP
Frances L. Edwards, MUP, PhD, CEM

January 2020

A publication of
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192-0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. 19-36	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Transportation, Terrorism and Crime: Deterrence, Disruption and Resilience		**5. Report Date** January 2020 **6. Performing Organization Code**
7. Authors Daniel C. Goodrich, MPA, CEM, MEP, https://orcid.org/0000-0002-8123-6554 Frances L. Edwards, MUP, PhD, CEM, https://orcid.org/0000-0002-0446-5556		**8. Performing Organization Report** CA-MTI-1896
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192-0219		**10. Work Unit No.** **11. Contract or Grant No.** 69A3551747127
12. Sponsoring Agency Name and Address U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology University Transportation Centers Program 1200 New Jersey Avenue, SE Washington, DC 20590		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code**
15. Supplemental Notes DOI: 10.31979/mti.2019.1896		

16. Abstract

Terrorists likely have adopted vehicle ramming as a tactic because it can be carried out by an individual (or "lone wolf terrorist"), and because the skills required are minimal (e.g. the ability to drive a car and determine locations for creating maximum carnage). Studies of terrorist activities against transportation assets have been conducted to help law enforcement agencies prepare their communities, create mitigation measures, conduct effective surveillance and respond quickly to attacks.

This study reviews current research on terrorist tactics against transportation assets, with an emphasis on vehicle ramming attacks. It evaluates some of the current attack strategies, and the possible mitigation or response tactics that may be effective in deterring attacks or saving lives in the event of an attack. It includes case studies that can be used as educational tools for understanding terrorist methodologies, as well as ordinary emergencies that might become a terrorist's blueprint.

17. Key Words Security, critical transportation, terrorism, transportation security, vehicle ramming	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 60	**22. Price**

Form DOT F 1700.7 (8-72)

Copyright © 2020
by **Mineta Transportation Institute**
All rights reserved

DOI: 10.31979/mti.2019.1896

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu

ACKNOWLEDGMENTS

The authors are grateful to the Federal Law Enforcement Training Center staff for requesting this study as an educational tool for their courses.

The authors thank Editing Press, for editorial services, as well as MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Graphic Designer Alverina Eka Weinardy; and Executive Administrative Assistant Jill Carter.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Terrorist activity in the United States has gone on for over one hundred years. Terrorist tactics have been used by anarchists, Ku Klux Klan, labor protestors, anti-war organizations, eco-terrorists and nationalist militia members, and most recently by Islamic jihadists. Law enforcement agencies have developed strategies and tactics for dealing with terrorist attacks against civilian populations and infrastructure, using vehicles as a weapon and as a target. Because terrorism ebbs and flows, much of the useful information developed during earlier terrorist attack cycles has been lost. Field level personnel have developed successful methods, but have not always written them down. Word-of-mouth training is lost through retirements.

This study investigated the existing literature that includes guidance on response to terrorist activities, including military manuals developed during wars. Useful open source manuals and documents are highlighted for future use.

The first step in successful counterterrorism is understanding the target, and what might be done to protect it. Transportation by its nature is an open system that has minimal protection. The length of the routes and the varied terrain make the development of a robust security plan challenging. Thousands of people freely get off and on transit vehicles every day with no screening. Thousands more use stations and ports for access to ferries and trains, creating further vulnerabilities. Tight budgets for public agencies have left critical transportation infrastructure with a maintenance backlog, leading to corrosion and missing parts that might contribute to worsening terrorist-induced damage.

The Transportation Research Board has noted that four strategies provide reasonable response to the terrorist threat. Materials and designs that heightened the likelihood of getting caught before completing the attack deter some perpetrators. Good lighting and well-placed cameras can assist security patrols in detection of potential attackers before they can act. A "see something, say something" campaign can involve the traveling public in surveillance of transportation facilities, leading to the interdiction of 9% of planned attacks in the US, according to Jenkins (2017). Robust barriers can deny access to potential criminals, while some technology – like camera recordings – might mitigate the damage by facilitating the rapid response to the scene of a disaster.

Security and protective measures come in multiple forms. In the past information about terrorist threats and attempts was considered highly classified. Law enforcement agencies at different levels of government and in different jurisdictions did not share terrorism intelligence with each other, leading to segmented knowledge and a failure to "connect the dots." A recent development to overcome this challenge is the fusion center, where representatives from multiple jurisdictions with security clearances meet to share information on suspicious activity and criminal behavior that can help to create a pattern that can be investigated. Challenges include determining who will be sponsored for the security clearance from other agencies, like fire department and public health departments, who might have or need the intelligence.[1]

The Department of Homeland Security has led in developing guidebooks and training

courses to collect and preserve professional knowledge, and share it among appropriate agencies. This includes case studies of actual events that demonstrate successful tactics, or provide critiques of less successful tactics that never the less lead to a better understanding of terrorist behaviors. This research added military manuals from wars of the 20th century that demonstrate terrorist and counterterrorist tactics that can be used against transportation vehicles and infrastructure.

Since 2014 vehicle ramming attacks have risen in popularity among Islamic jihadists. The ISIS webzine exhorted its global followers to use cars and trucks "as mowing machines" to cut down the infidels. Lone wolf terrorists (individuals acting alone) took up the challenge. The report documents 17 vehicle ramming attacks around the world between 2014 and 2017, including the deadliest attack, which was in Nice, France in 2016, demonstrating that the tactic had also been adopted by anti-jihadists, Chinese separatists, and even an "in-cell" male protesting his inability to get dates.

The report includes a section that reviews the most common technologies for protecting assets and the related trends. It discusses in some detail the use of cameras, fencing and lighting for deterrence, detection and denial of access.

The last segment of the report provides detailed case studies of three "ordinary emergencies" that could become blueprints for terrorist attacks. The events include the Baltimore Tunnel Fire of 2001, the San Jose Transit Mall collapse of 1992, the AT&T denial of service attack in south Santa Clara County in 2009, and one actual terrorist event, the New York City vehicle ramming attack of 2017.

The major findings are:

1. Terrorists continue to find transportation an attractive target and weapon. A self-motivated machine can be turned into a self-destructive machine by redirecting its energy.

2. A car or truck is a lethal weapon that is easily acquired and able to be used by most people. Vehicle ramming is a recent variation on the theme of vehicles as weapons. Pedestrians on any street, and crowds at large gatherings, make easy targets. ISIS advocated using the car or truck as a "mowing machine."

3. Terrorist attack modalities have changed little over the last one hundred years, from Buda's Wagon to the attacks in Belgium. Field-level lessons and tactics for deterring and interdicting terrorist activities have been developed and then lost because they were not written down, demonstrating the need for better documentation of methods used successfully against specific types of attacks. As law enforcement personnel become more adept at responding to one modality, terrorists rotate their methods, and responders must use lessons learned in earlier time to respond successfully to the tactic when it is reintroduced.

4. Law enforcement personnel became adept at infiltrating and monitoring terrorist cells. This drove the terrorists to using smaller groups, and ultimately the "lone wolf."

They have reorganized to keep personnel dispersed, using webzines to promulgate radicalization and promote tactical advice. While using lone wolf tactics does not prevent the orchestration of attacks, it does reduce the capacity to inflict carnage.

The report concludes with arguments for cost/benefit thinking in choosing response strategies, valuing dual use deterrence like lighting that protects a parking lot while illuminating sensitive transit control systems, and placing the focus on safety of passengers and staff of transportation agencies. A glossary of unique terms concludes the research material.

I. INTRODUCTION

Terrorist activity in the United States has gone on for over one hundred years. Terrorist tactics have been used by anarchists, Ku Klux Klan, labor protestors, anti-war organizations, eco-terrorists and nationalist militia members, and most recently by Islamic jihadists. Law enforcement agencies have developed strategies and tactics for dealing with terrorist attacks against civilian populations and infrastructure, using vehicles as a weapon and as a target. Because terrorism ebbs and flows, much of the useful information developed during earlier terrorist attack cycles has been lost. Field level personnel have developed successful methods, but have not always written them down. Word-of-mouth training is lost through retirements.

Federal law enforcement officers are confronted with the possibility of terrorist and criminal activity against transportation assets, yet there is little practical academic material developed to address their training in this complex field. While much has been written about particular instances of terrorist attacks on transportation, notably the catastrophic attacks by airplane hijacking of 9/11, and on the Madrid (3/11/04), London (7/7/05) and Moscow (3/29/10) commuter systems, little open source information has been developed to systematically examine the elements of successful counter-terrorism tactics and preventive strategies for transportation systems of the 21st century. Jenkins' work forms an important part of this small body of open source transportation-focused literature.

One problem is that many lessons learned about attacks on transportation in earlier periods of civil unrest and warfare have been lost through lack of historical knowledge or disuse. The purpose of this paper is to gather together some historical knowledge with a review of current practice, and to examine the contemporary challenges facing law enforcement officers engaged in counter-terrorism and crime prevention efforts in defense of transportation assets. As the mode of attack changes from sophisticated plans attempted by networks to simple attacks attempted by lone-wolf terrorists, and from the use of complex explosive devices to the use of knives and trucks,[2] this older tactical knowledge may be more useful for creating resilient systems than employing sophisticated technological systems.

RESEARCH QUESTION

What do federal law enforcement personnel need to know about current transportation security challenges, available resources and future concerns?

II. BACKGROUND

Transit and transportation have long been targets of terrorists. Historical examples have been well-documented, including the use of a horse-drawn wagon for an anarchist bombing of Wall Street in 1920,[3] the crucial role of train sabotage in World War II[4] and the many attacks worldwide on various forms of surface transportation in the 1990s[5] such as the Sarin attack in the Tokyo subway and the many attacks against busses around the world. After 9/11 the role of transportation in terrorist attacks drew international news coverage and extensive scholarly writing, both as an attack mode (hijacked aircraft used in the 9/11 attack) and as a target (commuter rail systems in the Madrid , London and Moscow bombings.[6]

These events heightened interest in teaching techniques for countering terrorism to the law enforcement agencies responsible for providing protection and security services to transit and transportation agencies. Traditional methods of security, such as fences, lighting and surveillance cameras, have been augmented with facial recognition software, bomb-sniffing dogs and the use of random security sweeps by the Transportation Security Agency (TSA) at transit and transportation hubs across America, under the Visible Intermodal Prevention and Response (VIPR) program.[7]

PHYSICAL SECURITY AND CAMERAS

Physical security for transportation assets is created by layers of surveillance, including human and canine guards, fences and cameras. The cameras may be monitored in real-time, or they may be recording-only cameras, as in the London subway during the 7/7/05 attacks[8], after which the cameras' images were used to identify the bombers.[9] The London camera system, which was initiated in the 1990s as an anti-crime measure, now consists of six million installations,[10] too many for humans to monitor in real time. The American Civil Liberties Union (ACLU) has questioned whether the cameras are worth their financial cost, citing studies that suggest that they just move crime to areas without cameras.[11] An attempted terror attack in London in June 2007 was disrupted by "human observation and common sense," while an attempted attack in Glasgow was stopped by a physical barrier, not information from the cameras.[12]

Government camera systems in London and a mixture of public and private camera systems in New York are ubiquitous in these cities. The Las Vegas Strip is covered by privately-owned casino cameras. Across America, shopping malls, retail stores, mass transit stations and vehicles, and many other public places routinely record video of patrons and transactions, primarily with the purpose of providing evidence when a crime occurs rather than for real-time detection. As resolution of the cameras improves, increased bandwidth becomes available, and improvements are seen in the processing power of computers and in the effectiveness of software for facial recognition and item recognition, these surveillance systems will become still more common, providing heightened surveillance against criminal acts of all kinds, but also less privacy everywhere.[13]

Some cameras are staffed, but the level of attention paid by the operator will depend on the level of training and supervision provided[14]. Some camera systems both record and are monitored by a human, and some even use facial recognition software, especially in

high threat areas.[15] However, cameras are not the only means of preventing terrorism; Jenkins[16] notes that 9% of terrorist attacks that have been attempted were prevented by observant bystanders who notified security personnel of suspicious packages.

Even as surveillance has increased in big cities and sensitive areas, the task of finding perpetrators in advance of their commission of a crime has become more complex. In previous times of unrest, attacks were planned by groups at physical meetings. Meetings by the German Bund in the 1930s, the Ku Klux Klan in the 1950s and 1960s, the Black Panthers and anti-war groups in the 1960s and 1970s, eco-terrorists and the militia movement in the 1990s, and terrorist cells in the 1990s and early 2000s provided opportunities for covert operations by the Federal Bureau of Investigation (FBI) and other law enforcement groups. Recent evolutions in terrorist organizations have resulted in the internet becoming the source for technical and tactical information, leaving individuals to operate independently or in very small teams that make infiltration by law enforcement personnel impossible.

INTERNET PUBLICATIONS

Radicalization through internet sites has become common, with ISIS's magazine *Rumiyah* and its predecessor *Dabiq,* and Al Qaeda's magazine *Inspire*, being available on the internet internationally. Detailed instructions for bomb-making and attack planning are readily available on multiple sites,[17] including YouTube. Books detailing strategies for committing crime, like Rex Feral's *Hit Man*, originating as a detailed fiction novel but presented as a how-to manual, have gone out of press following lawsuits resulting from the use of these books as guides in the committing of actual crimes. Since the publishers no longer protected the copyright, there has been a proliferation of this old material on the internet. People who know the right keywords to search can get ready access to information for terrorist and criminal activities. This could include using "kitchen improvised" for finding homemade bomb-making instructions. Military manuals like the Department of the Army's *Boobytraps* (FM 5-31)[18] give access to booby-trapping information, while TM31-200-1[19] and TM 31-210[20] give access to improvised munitions information. TM 31-210 was one source for the information in William Powell's *The Anarchist Cookbook.* Chemistry textbooks and manufacturers' usage guides like DuPont's *Blaster's Manual*[21] are also among the items that are readily available on the internet.

This proliferation of terrorist-usable information on the internet has aided in the planning of violence, and internet-based ideological and religious material may encourage violence;[22] however, these website visits can also be used to track potential attackers. Metadata collection at the national level and warrant-based access to IP activity has facilitated apprehension of terrorists. The UN Office on Drugs and Crime has developed protocols to assist law enforcement with collecting digital evidence that is admissible in court proceedings, in order to support prosecution with information about the online activities of those accused of terrorism and other crime.[23] In some cases, the evidence of internet activity may not be used in court, but it can nevertheless expose potential terrorists, increasing the paranoia of potential co-conspirators and thereby possibly creating deterrence.

ROAD AND RAIL RIGHT-OF-WAY

A further complication in securing transportation infrastructure is the multiplicity of uses to which roads, highways and bridges are often put. Local streets are frequently the sites of conduit for multiple public utilities. It is common for sewer pipes, natural gas lines and water pipes to be laid in trenches dug into the verge of an urban road, and conduits for electrical lines, telephone lines and fiber optic cables is run at the top of the trench. Highways may also provide shared right-of-way for long distance utilities and pipelines. One major highway bridge in a western state carries a road, a railroad, a natural gas pipeline, electrical lines and communications system lines. Its destruction or compromise would have an impact throughout the region for all of these uses, as there is no immediate workaround available in this isolated area for providing access without this bridge.

Disruption of a road or utilities can have cascading effects that can cripple a community. An explosion on the road surface may rupture utility connections buried in the trench, denying normal telephone and internet connections to hospitals and emergency services, as well as to the 9-1-1 system. Damage to the bridge structure may destroy the rail and utility connections that it carries. Intentional flooding of the trench to damage or destroy the utilities can wash away the underlying geological support of the road (sand, gravel) and cause the street surface to collapse into a cavity created by the flowing water. Real-world case studies of such events are given at the end of the paper.

Rail lines also provide a route of travel for ancillary activities. Historically the telegraph lines and then the telephone lines followed the rails, along with electrical lines needed to operate critical signals and switches. Fiber optic cables and Wi-Fi have since been incorporated to facilitate communications, signaling and switches. Positive train control, an advanced system designed to prevent collisions, prevent speed-related derailments, and prevent trains from running on the wrong tracks against signals,[24] relies on radio signals that require electrically-powered repeaters. Loss of these utilities can result in the inability to operate signals and switches, shutting down rail lines. More recently hazardous materials pipelines for natural gas and petroleum products have also shared the railroad right-of-way. Damage to a rail line can cause the related utility lines and pipelines to be damaged, while sabotage or destruction of the utilities might also damage the railroad and its ability to function.

III. FINDINGS: TRANSPORTATION SECURITY CHALLENGES, RESOURCES AND FUTURE CONCERNS

A careful study of transportation security has revealed a variety of concerns that are common across all transportation modes. These concerns include: the nature of transportation vehicles and their technology; the nature of transportation infrastructure and its maintenance; human factors; the nature of security and protective measures; and historical knowledge, its usefulness and its loss. The Findings section ends with an overview of vehicle ramming attacks as terrorist tactics.

THE NATURE OF TRANSPORTATION VEHICLES AND TECHNOLOGY

Transportation vehicles by design are self-propelled, therefore they can be self-destructive. Whether it is a bus, light rail, an airplane or a ship, its own power can be turned against it. Loss of control over the direction and speed of the vehicle through mechanical failure, sabotage or operator intent can cause a catastrophic accident. A variety of recent accidents can be taken as models of what could happen through intentional disruption in a terror attack. The tourist "duck bus" crash in Seattle on the Aurora Bridge, that left four people dead, two critically injured and sixteen others in the emergency room, was due to vehicle failure,[25] but it demonstrated the chaos and disruption created when a vehicle travels uncontrolled through dense traffic and hits another vehicle, in this case a tour bus. A tour bus accident in San Francisco's heavily populated Union Square shopping district left four people in critical condition and many more injured after it "hit nearly everything in its path for two city blocks,"[26] including two pedestrians and a bicyclist, multiple parked cars, and power poles for the city's electric buses.[27] The driver claimed that the brakes failed, but the investigation pointed to operator error, mistaking the gas pedal for the brakes. The bus was traveling 40 mph when the driver intentionally stopped by hitting a construction scaffolding.[28]

Rail also presents a vulnerable transportation system which could be exploited for terrorist purposes. The accidental Amtrak/CSX train crash in South Carolina in 2018 presents a model of this vulnerability. Although transportation systems incorporate multiple levels of safety devices, these can be overridden or damaged. During a period when the rail system's normal signal system was not operating, CSX railroad was dispatching its own trains. Its freight train was assigned to a track that was later also assigned to an Amtrak passenger train that collided with the stopped freight train.[29] Because the signals were not working the Amtrak train had no warning of the presence of the CSX freight train. Two crew members in the Amtrak engine were killed by the 40 mph collision, and 116 passengers were injured. Thousands of gallons of potentially flammable fuel were spilled.[30] Reports of the accident could provide a blueprint for terrorist attacks on rail by disrupting signaling systems. As Battelle noted in a recent 2018 study, "Signal errors can sometime result in collisions or derailments when a malfunctioning signal sends a train down the wrong track at the wrong time."[31]

Points of vulnerability in rail systems include a variety of safety mechanisms, such as dispatching, signaling and remote switching, which rely for their operation on radio transmission and computer coordination and which can therefore be subject to disruption and cyber-attack. Recently, a system called Positive Train Control (PTC) has been

developed, which the Rail Safety Improvement Act of 2008 (RISA) requires on all main lines for Class 1 railroads. It uses GPS to monitor the train's location, to prevent trains from entering unsafe areas. It can trigger the brakes remotely if the train is traveling too fast, or is about to enter an unsafe area, such as where the track is assigned to another train. PTC integrates signals, switching and crossing gates while trains are operating;[32] using a radio-based technology to connect to the controlling computer. The train records information about its speed and location which is then sent to "central control systems using wireless signals."[33] The intent is to provide safety by warning the engineer of speed or location issues, and applying the brakes automatically if the engineer does not take action".[34]

There were delays in PTC installation along the Amtrak Northeast Corridor, due to problems in coordination with the Federal Communications Commission over the assignment of radio frequencies to the trains in crowded urban areas. By the time of the 2018 Amtrak crash in South Carolina, the system still had not been fully implemented. This lack of PTC, three years after the systems were mandated, may have been to blame for the crash.[35]

The PTC is an example of a Supervisory Control and Data Acquisition (SCADA) system, also known as an Industrial Control System (ICS). These systems are operated by computer software that interprets signals from a source and creates a response. SCADA can also be used to manage and control other aspects of transportation operations, such as the signal systems and switching systems. This software can be tampered with to change the meaning of the signal or the response to the signal. Indeed, there is precedent for this; the Stuxnet computer virus, which was used to damage the Iranian nuclear program's uranium-purifying centrifuges, worked through interference with the SCADA system controlling the centrifuges, causing them to operate improperly.[36] Stuxnet is only the most famous of many SCADA attacks, including Industroyer and CrashOverRide malware used against the Ukraine's power grid in December 2016, for example.[37]

A serious vulnerability of these rail transportation safety features is that they mostly operate through radio frequencies, which means that they are vulnerable to radio frequency jamming. Jamming is illegal, and can be detected, but may be effective for short periods of time. A low wattage signal, generated in close proximity to the intended target, can be effective and difficult to detect.

Additional system vulnerabilities are rail systems' susceptibility to negative track conditions, such as debris on the tracks, and the failure of equipment through poor maintenance or intentional damage.[38] Rail service can also be disrupted by derailing and other forms of infrastructure sabotage.

Providing complete protection of rail assets is not possible. Rail lines stretch for thousands of miles. Military research has demonstrated that it takes a full battalion of military personnel (600 personnel) to secure just 100 km (62 miles) of rail line, with 2 guards per kilometer, on three 8-hour shifts per day. In addition, especially vulnerable parts of the infrastructure like trusses, bridges and tunnels would demand enhanced guarding. Roving patrols and an available response force would also be required to provide full rail system security. It has been estimated that staffing all these positions will require at least 800 personnel per 100 km.[39]

Information which terrorists and criminals could use for developing attacks on transportation systems is available from various sources. Bulletins are circulated among heavy rail operators concerning security issues, including instances of tampering with switching systems. There is also public disclosure through government procurement systems of the specific equipment that was purchased, including information technology systems. Security systems may be revealed during public hearings on related issues, like procurement costs or system efficiency. Al Queda's *Inspire Magazine* even quoted information from Government Accountability Office (GAO) reports critiquing security programs.[40] Federal departments may disclose information in manuals and guides which terrorists could use for creating disruptive activities.[41] Public agencies may announce the acquisition of new sensors and communications systems in order to promote feelings of security among the public.

Freight rail is another point of vulnerability. It operates using the same systems as passenger rail, but its disruption may have more severe ramifications for an area or region than the disruption of commuter service. Freight rail in the United States is the major transportation conduit for heavy assets for industry, international trade and defense. Unlike the public Amtrak system, freight rail systems are generally privately-owned, leading to lack of coordination of security precautions across all companies sharing the system.

Military tactics have been developed for disruptive effect and denial of service on the rail system, not to incapacitate permanently.[42] Significant economic impact can be gained by delaying deliveries of critical components. A civilian accident demonstrates the impact of schedule disruption on the economy. For example, land slippage at the construction site of a tunnel in Rastatt, Germany closed its principal north-south railway that links ports at Rotterdam, Hamburg and Antwerp. As a result, 200 freight trains were stranded on the tracks, with losses to industry estimated at millions of Euros per week. Residual capacity on possible alternate rail routes was scarce during this time due to construction activities. Road alternatives for trucks to replace trains were impacted at border crossings due to truck inspection requirements, with Switzerland and Italy especially hard hit by long delays.[43]

THE NATURE OF INFRASTRUCTURE AND ITS MAINTENANCE

Poor maintenance of transportation facilities creates opportunities for sabotage and other terrorist acts against weakened infrastructure. While deficiencies in road and bridge maintenance are frequently noted,[44] there are also deficiencies in other elements of transportation system upkeep.

In 2013, the Federal Transit Administration estimated that there's an eighty-six-billion-dollar backlog in deferred maintenance on the nation's rail and bus lines. The American Society of Civil Engineers, which gives America's over-all infrastructure a grade of D-plus, has said that we would need to spend $3.6 trillion by 2020 to bring it up to snuff.[45]

Metropolitan New Orleans' experience with Hurricane Katrina showed how a "normal disaster" was worsened by the poor maintenance of the closely interrelated drainage infrastructure in the area, with cascading effects. Leavitt and Kiefer note that the failure of the levees led to the pumps being overwhelmed, and roads being inundated and washed away.[46] Without adequate security, similar results could also be caused deliberately through sabotage of the

pumps during storm conditions.

Stronger enforcement of building code regulations and stricter and more thorough bridge inspections could provide greater security for public infrastructure. Erosion prevention through regular maintenance measures as simple as painting could prevent "normal disasters" from leading to catastrophic failures. Rioja suggests that the economic rate of return (ERR) for highway maintenance investments in the United States is 25-38%, taking into account the value of full functionality of the road.[47] Analysts typically look at the benefits of road maintenance to users realized in lower costs for car repairs and shorter and less disrupted commutes.[48]

When the value of security is added to safety and economic impact captured in traditional models, the rate of return would be even higher. Consider the value of avoiding crises such as the collapse of the I-35 bridge in Minneapolis in 2002 that killed 13 people and injured 145 people. The National Transportation Safety Board (NTSB) determined that the primary cause of the collapse was a design flaw in the gusset plates, but years of inspections had not recognized this weakness, and the eventual proximate cause of the collapse was the loading of the bridge with construction equipment and supplies being used for a renovation project. This extra load during rush hour traffic stressed the plates, causing a catastrophic failure of the western span.[49]

While this event was due to poor evaluation of the bridge's design capacity, an intentional overloading of a bridge could be created deliberately by terrorists. The National Bridge Inventory of the Federal Highway Administration[50] and the grade crossing numbers of the Federal Railway Administration are published annually, and provide evaluation of the conditions of highway and railroad bridges for the purpose of distributing maintenance funding[51]. These lists could guide terrorists to bridges in weakened condition, facilitating a collapse attack. This suggests that heightened surveillance of listed bridges could be an important deterrent to tampering and terrorism.

HUMAN FACTORS

The Transportation Research Board (TRB) has highlighted four elements of transportation security, which can be used to evaluate the effectiveness of security programs against human criminal or terrorist action: deterrence, detection, denial of access, and mitigation.[52] The design and extent of the transportation infrastructure may make it impossible to use all four elements on every asset, but in any case some combination of the four approaches can be used to enhance the security of transportation.

Deterrence

Active surveillance with staffed cameras backed up by a rapid response force, selective passenger screening, and bomb sniffing dogs are all designed to deter attacks by making their planning and execution too difficult. Fences, walls, guarded entrances and alarms may provide deterrence by protecting the most valuable or most newsworthy elements of a target, reducing the value of an attack. For example, Israel has long employed the rapid clean-up and restoration of bus bombing sites, devaluing the psychological impact on the

civilian population.[53]

Preventative measures taken in advance are needed to successfully deter terror attacks. This includes the promotion of awareness of terrorist tactics and methods among civilians, allowing them to more easily notice unusual circumstances and report them to local authorities. Such “see something, say something” programs have been an effective strategy in deterring and disrupting terrorist plots.[54]

Bus drivers are on the front line of protecting their passengers from criminal actions. One example shows how quick thinking can deter attacks on passengers. For example, one bus driver had a mentally disordered passenger draw a knife, threatening her and her passengers. The bus driver surreptitiously hit the panic button and pulled the bus to the curb. The knife-wielding passenger demanded that she drive on, but she told him that she was ahead of schedule, and that she would get in trouble if she got to the next stop early. Her quick thinking allowed time for the police to locate and board the bus, and disarm the passenger.

Other civilians can also do their part to promote safety. One dog walker successfully deterred a planned attack using improvised explosive devices (IEDs), when she called the local police about a “terrible odor” coming from a back yard that she walked passed each day. She had thought that it might be a meth lab, but investigation by the local code enforcement officer revealed that the back yard was filled with open containers of urine. Urea nitrate, a favorite explosive used by terrorist groups based in the Middle East, can be cheaply made by concentrating urine by exposure to sunlight. Her report led to revelation of a terrorist plan to make IEDs.[55]

In another case, a neighbor was curious about why some young men in her apartment building were receiving deliveries of large boxes labeled “medical glassware.” When she asked where they worked, the men said that they were trash collectors. In this case too, the woman suspected a meth lab and called the police. Investigation revealed that the men were setting up a system for making a biological warfare agent to release in the New York City subway system, a plot modeled on the 1995 Sarin nerve agent attack in Tokyo.[56]

Sometimes actions are only seen as suspicious in retrospect. After the 7/7/05 subway and bus bombings in London, a beauty supply operator contacted police to say that she might have been the source of the raw materials for the tri-acetone tri-peroxide (TATP) explosives used. She reported to the London Metropolitan Police that two men who resembled the bombers had come to her beauty supply shop a few days earlier, buying a large quantity of hair bleach and nail polish remover. When she asked them what they needed it for, they said that their sister was opening a beauty shop. She thought it odd that they wanted all that bleach, but no other hair products, and nail polish remover, but no nail polish or manicure products. When she heard the name of the explosive she was struck by the presence of peroxide in hair bleach and acetone in nail polish remover.[57]

The Department of Homeland Security (DHS) has created a program that is intended to develop awareness of possible terroristic uses of common household and hardware store items. The Bomb-making Materials Awareness Program (BMAP) is offered to police

departments and retail stores to explain how bombs can be created using readily available items like pool chemicals, fertilizer, irrigation pipe, screws, nails and wire. The program is intended to heighten the level of suspicion when someone buys an unusual combination of items. An example of such an unusual combination would be the purchase of lots of pipes and caps, but no connectors—materials used for making pipe bombs. The goal is to help retail clerks recognize when something is amiss and notify local law enforcement so that they can investigate.[58]

Detection

Detection is the second method for devaluing an attack. Detection may focus on interdicting the planning process, or on finding the device in advance of its deployment. Strange behavior at a transit station – such as sitting on the platform for long periods or taking photos of infrastructure – may signal attack planning. Detection may allow for evacuation, arrests, or bomb disposal in advance of detonation.[59]

Denial of Access

Denying attackers access to their target is the next aspect of security. Even after an attack has been planned, or even begun, the high value human or material target can be moved away from danger. The target may be placed behind additional levels of security that are harder to breach. Escape tunnels, safe rooms and changes to access protocols all fall into this category.[60]

Mitigation

Mitigation is the fourth strategy for heightened security. Even if an attack cannot be prevented, mitigation measures can be installed or implemented that thwart the purpose of the attack. The goal is to protect the primary target (human life), while perhaps allowing some damage to less-valuable elements of infrastructure. Bullet-resistant glass, rail car roofs designed to explode upward in an attack, and the redesign of potential hiding places for explosives, such as switching from solid to open-mesh refuse containers, can all lower the impact of an attack.[61] Increases in the speed of identification and interdiction of attackers can be achieved through facial recognition software, license plate readers and constantly changing passwords.

Physical security cannot prevent every attack or protect every target, but it can slow down the progress of an attack to allow the responders time for interdiction. Jenkins and Butterworth note the value of blocking pedestrianized roads with bollards, and blocking access to markets and festivals with trucks parked across the access road.[62] Locks, safes and fences are all ultimately able to be overcome by determined intruders, but it takes time, and that increases the probability of detection, which may enable a robust response to be implemented before the high value target is reached.

Cameras

Sometimes, strategies to deter, detect, deny access and mitigate may be based on false assumptions. For example, in the 1990s, the Bay Area Rapid Transit (BART) system installed what appeared to be surveillance cameras in many of its rail cars to deter crime against passengers. This widely publicized strategy backfired when a murder took place on a BART car in 2016, and passengers did not take cell phone footage of the shooting because they assumed that the BART cameras were working. It was later revealed that less than 25% of the cameras were functional, while the rest were "dummy" or faux cameras that did not record anything. Law enforcement investigators had to rely on station cameras to find pictures of the shooter,[63] who has never been identified.

Eric Swalwell, the local congressman, complained to the website SFGate, "I had assumed that every time I got on BART those cameras were rolling and someone was watching"; the website also reports that "he said he also wasn't aware that none of the onboard devices—there are four in each car—can be monitored remotely in real time, which would allow BART to better respond to unfolding emergencies."[64] This demonstrates a further widespread misconception about cameras, since most surveillance cameras are intended only for recording activities for use in identifying and prosecuting law breakers after the fact, not interdicting the event. This use was demonstrated in the 7/7/05 London bombings, in which the cameras did not prevent the attack but did allow the identification of the bombers.[65] BART promised that the new cars being installed between 2017 and 2021 would have working surveillance cameras. Indeed the new cars came equipped with 2,000 of them.[66]

Counter-terrorism funding has been used by some large transit agencies to provide cameras in all trains, stations and buses. For example, the Chicago Transit Authority has 23,000 cameras across its system. After 9/11, New York City's Metropolitan Transportation Authority has been outfitting all of its new buses and trains with working cameras, and San Francisco Municipal Transit Authority has cameras in all the buses, rail and cable cars.[67]

Sometimes cameras have multiple purposes. In San Jose, the traffic cameras can be reoriented from the traffic flow in the street to observe the level of water in the street during a flood. At Disneyland there are cameras whose primary purpose is the monitoring of the lines at rides in order to modify the operational tempo to better meet demand, but these same cameras can reveal crimes in progress or record the identity of someone who has committed a crime. The utility of monitored cameras for these purposes is limited by the person observing, as a security-oriented worker may not notice the back-up of waiting riders, while a ride-oriented worker may miss indications of someone committing a crime.

London's 2012 Summer Olympics saw an unprecedented level of surveillance for the city, designed to ensure the safety of the athletes and spectators at the games. Indeed, even the Olympic Games' mascots were dolls with one huge eye that "records everything."[68] Among the innovations introduced for the Olympics were "intelligent CCTV surveillance systems."[69] These CCTV systems are enabled through greater camera resolution, a wider range of lighting conditions, enhanced computer processing power and refinement of the software. Their constant operation demonstrates to would-be disrupters that the Olympic sites and activities are under constant surveillance by many specialists.[70] The responsiveness of the CCTV system is also enhanced by the addition of facial recognition

systems and license plate readers. In addition to CCTV, other security upgrades included new scanners, biometric ID cards, and disease tracking databases.

Under Piccadilly Circus in London, staff in a control center with 47 screens monitored the camera output 24 hours a day, every day during the Olympic Games, enabling the security team to view large areas of London in high definition. Three people worked on each 12-hour shift to monitor the 47 screens that gathered feeds from 120 cameras, both traditional and wireless, while DVRs recorded the video output. Not surprisingly, the staff stated that their biggest challenge was staying awake during the long shifts, which is a common problem in the security industry. The upgrade to the existing surveillance camera system of the City of Westminster (part of Greater London) cost £500,000, but was reputed to have improved the picture quality by 400%. The goals of the system were to monitor traffic, to prevent criminal activities, including non-violent ones like the sale of fake Olympic merchandise, and to prevent terrorist attacks on the venues that drew one million extra people to London during the games.[71] This technology was backed by a security force of more than 24,000 members, which is the largest mobilization of police and armed forces personnel in the United Kingdom since the Second World War.[72]

Intelligent surveillance camera systems allow operators to change from passive surveillance to active tracking of selected individuals in real time. Cameras can be linked to allow the monitor to skip from one camera to the next as a crime or suspicious event unfolds. While the technology for tracking an individual through computer-aided camera switching is still developing, this is a revolutionary development, because the cameras were previously primarily intended only for documentation rather than for the proactive tracking of a criminal in real time. Previously, attentive security personnel could choose to manually switch cameras to follow an individual as a crime unfolded, but this required a thorough knowledge of the facility and the camera angles in order to avoid losing the suspect in the blind spots of the camera system. The computer-aided tracking is more rapid and accurate.

NATURE OF SECURITY AND PROTECTIVE MEASURES

Urban environments offer many data collection opportunities, but generally the data collected is only analyzed by the agency collecting it. Law enforcement is a state's rights role under the 9th and 10th Amendments to the U.S. Constitution. Federal agencies and state/local law enforcement entities generally only collaborate on specific bases or activities, otherwise operating in separate law enforcement spheres. In the past, most federal law enforcement agencies operated under a "need to know" philosophy of information sharing with non-federal law enforcement agencies. Monitoring of infrastructure systems is performed by the owners independently, with each utility and agency monitoring its own infrastructure through its own security or law enforcement personnel. Only crimes or security compromises cause coordination among different law enforcement agencies, to generate mutual understanding of environments.

Fusion Centers and Information Sharing

In most metropolitan areas critical infrastructure agencies do not share information about

security issues across jurisdictions and infrastructures. “Fusion centers” were created after 9/11 in order to try to break down institutional barriers to information sharing, but some have been more successful than others. The DHS defines fusion centers as “a collaborative effort of two or more agencies that provide resources, expertise and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.”[73]

The 2011 revision of homeland security strategies, Presidential Policy Directive-8[74], recognized “critical transportation” as an element of critical infrastructure/key resources and as a core capability.[75] Presidential Policy Directive-21 designated 16 critical infrastructure sectors,[76] including the transportation systems sector.[77] Transportation’s seven sub-sectors, as shown in Figure 1, are part of the fusion center information sharing network. The concerns of a state’s transportation agencies may be represented in the state-level fusion center by the highway patrol agency for that state. Large transit agencies may be represented in the metropolitan fusion center by their internal law enforcement department, or by the agency with whom they contract for transit law enforcement services. Small agencies, private sector transportation entities, and other transportation sector members, such as pipeline operators and private shipping services (e.g., FedEx, UPS), may not be directly represented, and proactive outreach from federal, state or local law enforcement agencies may be needed in order to gather and disseminate critical threat information related to potential attacks and security measures.

The Transportation Systems Sector consists of seven key subsectors, or modes:

Aviation includes aircraft, air traffic control systems, and about 19,700 airports, heliports, and landing strips. Approximately 500 airports provide commercial aviation services at civil and joint-use military airports, heliports, and sea plane bases. In addition, the aviation mode includes commercial and recreational aircraft (manned and unmanned) and a wide-variety of support services, such as aircraft repair stations, fueling facilities, navigation aids, and flight schools.

Highway and Motor Carrier encompasses more than 4 million miles of roadway, more than 600,000 bridges, and more than 350 tunnels. Vehicles include trucks, including those carrying hazardous materials; other commercial vehicles, including commercial motor coaches and school buses; vehicle and driver licensing systems; traffic management systems; and cyber systems used for operational management.

Maritime Transportation System consists of about 95,000 miles of coastline, 361 ports, more than 25,000 miles of waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.

Mass Transit and Passenger Rail includes terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, heavy rail—also known as subways or metros—light rail, passenger rail, and vanpool/rideshare. Public transportation and passenger rail operations provided an estimated 10.8 billion passenger trips in 2014.

Pipeline Systems consist of more than 2.5 million miles of pipelines spanning the country and carrying nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. Above-ground assets, such as compressor stations and pumping stations, are also included.

Freight Rail consists of seven major carriers, hundreds of smaller railroads, over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives. An estimated 12,000 trains operate daily. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.

Postal and Shipping moves about 720 million letters and packages each day and includes large integrated carriers, regional and local courier services, mail services, mail management firms, and chartered and delivery services.

Figure 1. Critical Infrastructure – Transportation

Excerpt from Department of Homeland Security. (DHS). "Critical Infrastructure Sectors." No date. https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed October 12, 2018).

Divisions within law enforcement - among the federal, state and local levels block intelligence sharing and coordination for routine information. Fusion centers help with the sharing of information about multi-sector threats and serious terrorist or criminal threats, but cross-agency sharing is not the norm on a daily basis. Few agencies have the staffing to maintain a regular exchange of routine law enforcement information, and yet it is often the small out-of-place action that exposes an individual as conducting surveillance of potential targets or as acquiring dangerous materials. For a hypothetical example, if a local police agency noticed that the same car was stopped next to a local railway company's right-of-way every day for a week when the hazardous materials hauling train passed, this information may not be communicated to the railway company, despite being valuable information for them to know; if the car was legally parked, the occupant might be a train spotter looking for unique cars or company logos, but the occupant might also be a terrorist conducting surveillance to plan an attack on the train line. For another example, a customer buying only metal nuts and irrigation pipe and caps, and no connectors or bolts, might attract the attention of hardware store security, who might bring it to the attention of local law enforcement, but they in turn may not think it necessary to report to the fusion center; however, this too may turn out to be important, for while the customer might be lengthening the irrigation lines on his property and replacing nuts on the clamps, he might instead be building shrapnel-containing pipe bombs.

Professional Knowledge and Documentation

Law enforcement officers who are assigned to regular patrol areas, or "beats," become familiar with the routine activities of that area, and are therefore well-suited to recognizing when something is out of the ordinary. Training should encourage the patrol officers to document what they see that is unique and worrisome. The accumulation of many small discrepancies may be the key to recognizing and stopping criminal or terrorist activity. Poole, in his book *Last Hundred Yards,* noted the value of the expert knowledge of non-commissioned officers (NCOs) in the military. Commissioned officers document their work well through mandatory regular reports, but NCOs do not, so the next generation of NCOs has to relearn the routine actions that create success. NCOs often overlook resources for providing the details of managing a situation. Ground experience of field personnel allows them to accumulate critical operational knowledge, but it is seldom documented. As Poole writes, "Because NCO knowledge has not been systematically retrieved, the US Armed Forces have not learned as much about small unit tactics as they should have… The tragedy is that every time a seasoned NCO or Staff NCO leaves the service, much of what he has learned about situational detail and the tricks of the trade of tactical execution goes with him."[78]

There was a notable loss of tactical knowledge after World War I. During the Great War there was knowledge developed about military tactics like sniping, machine gun employment, and tactical troop movements in trenches, but this tactical knowledge was not retained.[79] Activities that are generally considered to be at the NCO level and below were poorly documented or not at all. At the end of the war American forces were radically downsized, leading to a loss of group memory and knowledge.[80]

Now that digital voice recorders and cell phone cameras are readily available to police patrol

officers, it would be easier to accumulate this knowledge, if patrol officers were encouraged to collect it on agency-owned devices. As they discover the unique characteristics of each neighborhood in which they operate, and the specific techniques that work best there, they could document what is normal, so that new criminal activities or terrorist activity might be more readily identified.

Crime runs in cycles, and old techniques re-emerge.[81] Older patrol officer knowledge, like NCO knowledge, is not well documented either and is often lost. This reality is shown clearly in the confidence games that recur periodically when the public has forgotten them, creating a new generation of vulnerable people being helped by a new generation of law enforcement officers that has to relearn investigative methods. Sometimes these schemes make use of new technology, like cell phone calls or internet e-mail contacts, while at their core remaining the same. For example, the Spanish Prisoner trick is now conducted on the internet.[82] These schemes can be quite long-lived; Ponzi schemes existed even before the 1920s when they got the name, and are still being used through investors like Bernie Madoff.[83]

In World War II the British High Command created a special army unit tasked with engaging in sabotage in occupied Europe, called the Special Operations Executive. Their *Secret Operations Manual* encouraged the members to think like a perpetrator of crime, to anticipate actions, and to interfere with economic and military activities through destruction of assets.[84] Their targets included anything of value to the war effort that can be attacked. Their role was to act as a constant irritant to make the Axis' position more difficult, and to strain their intelligence-gathering capabilities to lessen the likelihood of detection of SOE troops. The lesson for contemporary law enforcement agencies to draw from the SOE is the importance of collecting intelligence from the perspective of the adversary (think like a criminal), and to learn to look at things from the point of view of how to destroy them (their sabotage training).

HISTORY AND LESSONS LEARNED AND LOST

Failure to document knowledge as it is developed results in its loss. Later events require the same disaster experiences for the knowledge to be regained, at a considerable cost. For example, after the Loma Prieta earthquake of 1989 communities struggled with rehousing the survivors. Community collaborations with local non-profit agencies and the housing industry resulted in relatively rapid housing repair and the rehousing of the community members.[85] After the Northridge earthquake of 1994 the California Office of Emergency Services used the Loma Prieta lessons to rehouse and rebuild effectively.[86] Yet rehousing challenges in disasters like Hurricanes Katrina (2005), Matthew (2016) and Harvey (2017) required the recreation of knowledge about coordination and collaboration with non-profit organizations; while California documented its internal systems, other states did not take advantage of the knowledge developed in the successful management of California's two urban earthquakes, and did not incorporate it into their state emergency plans.

Similarly, Smithson wrote *Ataxia* in 2000 to capture the lessons learned from asymmetric warfare in Tokyo during the sarin attack of 1995, to inventory then-current American capabilities, and to compile data from 33 American cities with some terrorism response capabilities.[87] While this publication carefully documents emergency response information, emergency responders have not been exposed to it, so none of the knowledge was applied

to the 9/11 attacks in New York City. In contrast, the Arlington Fire Department used the Incident Command System (ICS) in responding to the simultaneous attack at the Pentagon, an acknowledged best practice from numerous wildland fires and the Northridge earthquake, which was documented in *Ataxia.* The result was an efficient response to the crash,[88] leading to the National Incident Management System (NIMS) being based on ICS.[89]

Key people in any organization, whether military NCOs or beat patrol officers, develop deep practical knowledge, experience and understanding of their jobs, but when they leave this field-level knowledge can easily be lost. Documentation of successful strategies, and their incorporation into routine training, can keep the knowledge base growing, and provide a basis for developing successful responses to new challenges, including terrorist attacks on transportation assets.

VEHICLE RAMMING ATTACKS SINCE 2014

Jenkins and Butterworth have found that vehicle ramming attacks are on the rise. There have been 78 terrorist attacks using vehicles as weapons since 1973, but the frequency has increased markedly in recent years. In the 34 years from 1973 to 2007 there were 16 attacks; in the next eight years from 2008 to 2016 there were 32 attacks; and from 2017 to April of 2018, there were 30 attacks in only 16 months. The lethality of the attacks is generally increasing as well, with 43 killed in China in 2014, and 86 people killed in Nice, France in 2016, the largest number ever killed in one vehicle attack. Jenkins and Butterworth estimate that even without counting the Nice attack there are now on average 4 fatalities per vehicle ramming event, whereas between 1973 and 2015 there was on average less than one fatality per event. Injuries are usually in the double digits, but at the high end, in the China attack over 90 were injured, and in Nice 434 people were injured.[90]

Going back to ancient times, terrorist tactics were based on recruiting members for cells, and in the twentieth century on the development of complex IEDs and intricate plots. After 9/11, when the worldwide security apparatus was increased, jihadist terrorist organizations turned instead towards the use of slick publications on the internet, as noted above, to encourage individual terrorism. In 2010, Al Qaeda's online webzine *Inspire* featured an article, "The Ultimate Mowing Machine," that encouraged its followers to use pick-up trucks "to mow down the enemies of Allah."[91] By 2014, ISIS was encouraging its followers to run over infidels with their cars, in a list of lethal actions that could be carried out without traditional weapons.

Table 1. TSA List of Vehicle Ramming Attacks, 2014–2017

Attacks	Casualties
4/2017, Stockholm, Sweden (truck rammed a department store in the city center)	4 killed, 15 injured
3/2017 London, England (car rammed pedestrians on Westminster Bridge)	6 killed (including attacker), 50 injured
1/2017, Jerusalem, Israel (truck rammed military personnel near a popular promenade	5 killed (including attacker), 15 injured
12/2016, Berlin, Germany (truck rammed pedestrians at outdoor Christmas market)	12 killed, 56 injured
11/2016, Columbus, OH (car rammed pedestrians at Ohio State University)	1 killed (attacker), 11 injured
10/2016, Vienna, Austria (car rammed pedestrians on a busy street)	None
7/2016, Nice, France (truck rammed pedestrians during Bastille Day fireworks display)	87 killed (including attacker), 434 injured
1/2016, Valence, France (car rammed military personnel guarding a mosque)	1 injured
6/2015, Lyon, France (van rammed gas cylinders at gas factory)	2 injured
6/2015, Graz, Austria (car rammed pedestrians in the city center)	3 killed, 36 injured
12/2014, Nantes, France (van rammed pedestrians at Christmas market)	1 killed, 10 injured (including attacker)
12/2014, Dijon, France (car rammed pedestrians throughout the city)	11 injured
11/2014, Jerusalem, Israel (van rammed pedestrians at light rail station)	4 killed (including attacker), 13 injured
10/2014, Jerusalem, Israel (car rammed into pedestrians at light rail station)	3 killed (including attacker), 7 injured
10/2014, Quebec, Canada (car rammed military personnel in shopping center parking lot)	2 killed (including attacker), 1 injured
8/2014, Jerusalem, Israel (tractor rammed pedestrians and a public bus)	2 killed (including attacker), 5 injured
5/2014, Xinjiang, China (two sports utility vehicles rammed pedestrians in street market; attackers also threw explosives from vehicles)	43 killed (including 4 attackers), 90+ injured

Source: TSA, Office of Security Policy and Industry. *(U) Vehicle Ramming Attacks: Threat Landscape, Indicators, and Countermeasures.* Washington, DC: TSA, 2017. https://info.publicintelligence.net/TSA-VehicleRamming.pdf (accessed January 15, 2019).

Table 2. 2017–2018 Vehicle Ramming Attacks

Attacks	Casualties
4/2018, Toronto, Canada (rented van driven into pedestrians in North York Centre Business District for 2.2 km)	10 killed, 16 injured
10/2017, New York City (rented Home Depot pick-up truck driven 1 mile on Hudson River Greenway limited access bike trail, hitting bicyclists and pedestrians)	8 killed, 11 injured
8/2017, Barcelona (van driven into pedestrians on Las Ramblas, a crowded tourist boulevard)	13 killed, 130 injured; attacker was killed by police later
6/2017, London (van driven into pedestrians on London Bridge; terrorists ran to Borough Market and began stabbing people)	11 killed (including 3 attackers), 48 injured (including 4 unarmed police officers who intervened)

Sources: BBC News. “London attack: police ‘know identities of killers’.” June 5, 2017. https://www.bbc.co.uk/news/uk-40155451 (accessed June 5, 1018). Burgen, Steven and Ian Cobain, I. (2017). Barcelona attack: four suspects face court after van driver is shot dead. *The Guardian.* August 22. https://www.theguardian.com/world/2017/aug/21/police-searching-barcelona-van-driver-shoot-man (accessed June 15, 2018). Mueller, Benjamin, William Rashbaum, Al Baker. “Terror attack kills 8 and injures 11 in Manhattan.” *The New York Times.* October31, 2017. (accessed June 25, 2019). Tait, Melissa. Toronto van attack: How you can help and what we know so far. *The Globe and Mail.* April 23, 2018. https://www.theglobeandmail.com/canada/toronto/article-toronto-van-attack-what-we-know-so-far/ (accessed June 15, 2018).

The vehicle ramming attacks have often been perpetrated by “lone wolf” or “stray dog” terrorists with a variety of motivations, who create a plan, obtain a vehicle and commit the crime with no outside assistance. The 17 ramming attacks identified by TSA in Table I are mostly lone wolf attacks. Of the four more recent vehicle jamming events listed in Table 2, only the Barcelona attack seems to have been backed by a terrorist cell.

Most Deadly: Nice, France, July 2016

Jenkins and Butterworth point out that the Nice event was the most lethal of the vehicle ramming attacks to date, killing 86 people.[92] The attack occurred on Bastille Day (July 14), a summer holiday enjoyed by many French citizens. The sea front in Nice is a favorite gathering spot for watching the celebratory fireworks. Local officials created a security barrier around the Promenade des Anglais for the safety of the pedestrians strolling along it, but there was a failure in the security cordon, and a rented white cargo truck driven by a Tunisian was able to gain access to the water front street crowded with pedestrians. It initially traveled in the direction of the airport. Half an hour later it turned around and headed for the crowd, breaching the security barriers. After the driver would not stop, police fired on the vehicle and it sped up. For 2 km it zigzagged through the crowd, mowing people down. The police brought the truck to a stop, and then the driver began firing on police with a pistol. The driver was then shot through the windshield of the truck and killed.[93]

In response to the attack, 12,000 reservists were summoned to Nice, and citizens were asked to join the reserves. France’s terror alert level was raised to the highest level.[94] The dead and injured were from 19 different nations.[95] The injured were taken to the local university hospital, and 84 people died at the scene of the attack, while one died in the hospital.[96] Ultimately 434 people were treated for injuries related to the truck ramming.[97]

While the truck driver did not leave any message, Islamic State claimed that he had been one of their followers, and had carried out the attack “in response to calls to target the citizens of the coalition that is fighting the Islamic State.”[98]

IV. ANALYSIS

CAMERAS

Since the London 2012 Olympics, new approaches to transportation security have included more technology, used in various ways.

London's cameras provide beneficial information to law enforcement because they are actively staffed around the clock. Because of its expense, however, not many communities can afford such a comprehensive staffing system.

Some communities and transit organizations have cameras that record activities on the system, without an active monitoring force. This recorded and date/time-stamped information can be useful in tracing the movement of criminals, or identifying perpetrators after a criminal or terrorist act. The London subway and bus bombing in July 2005 was recorded, enabling investigators to identify the bombers, and then trace their steps from their original trips on the subway lines[99]. However, it is important to communicate to the riding public that the cameras will not trigger an immediate law enforcement response.

The length of video storage time is also an important factor when determining how valuable the recordings will be, and how they can be used. If the recordings are monitored live, it may be acceptable for them to be erased every 24 hours. This saves on cost for hard drive space, for indexing and for storage. Unmonitored recordings may need to be kept longer, since its value is retrospective after a crime has been committed. It may be days or even weeks before a victim and the investigating law enforcement department recognize the evidentiary or investigative value of the recordings.

FENCING

Fencing is another popular method for enhancing security. Fencing material can be selected to provide seclusion for the asset, such as rail equipment or parked buses. It may also be selected to provide a physical barrier without a visual barrier. Chain link fencing allows for easier observation of activity behind the fence by patrol vehicles, which may deter crime inside the fence.

Fencing does not provide perfect protection for the passengers or resources kept behind it. However, fencing does slow down someone seeking illicit access, because they have to pause to breech the fence by cutting the material or scaling it. Their action makes their criminal intent obvious to observers, during which time they may be observed and stopped. Fencing also channels access to the property, limiting the space that has to be regularly guarded to the access point.

Layered defense can be based on a foundation of fencing, to be augmented when more valuable assets or greater threats exist. For one example, guard dogs can be brought in for periods of heightened concern. For another, cameras can be installed along the fence which typically only record, but that can be monitored in times of increased sensitivity.

LIGHTING

The value of lighting is that it enables facility users to have more situational awareness of their surroundings from twilight to sunrise. It also enhances the ability of patrol personnel to observe activities within the facility. The placement, number and brightness of the light fixtures can be adjusted based on cost/benefit analysis of its relative deterrent factor. More light is needed in high crime areas, when high value assets are being stored, or to prevent trips and falls in uneven terrain. Routine lighting of paved walkways can be lower in safe areas. Low lighting creates shadows which provide hiding places for criminals and terrorists. However, a lack of lighting can also be a security option, as it blinds the criminal, while patrol officers can be issued night vision equipment. Ambient lighting can be enough for criminals to see their way around, yet not provide enough light for them to be revealed to routine patrol, so in general low lighting should be avoided.

Light has two on-going costs which may influence the choice of placement and brightness: electricity costs and bulb replacement costs. New technology using LED bulbs, however, both lessen the operating cost for electricity, and lengthen the time between bulb replacements. Many systems also permit the operator to lower the lights at low usage times, and increase the brightness when there is more pedestrian or vehicular traffic.

If cameras are being used, the lighting placement and brightness will have to be coordinated with the camera lens quality, to ensure that the light source does not reflect back onto the lens. Care must be taken in the selection of the lighting source and its color spectrum, as some lighting can render some colors invisible to the camera, even with newer technology. Systems must be tested to select the proper combination of light and camera. Choices of how to light fence lines to enhance patrol effectiveness should be determined by the anticipated threat being defended against and the terrain.

Light bulbs are generally made of glass, and so are inherently vulnerable to breakage by projectiles. They can also be blacked out with spray paint. Cages can be installed to protect the bulbs, but these can also dampen illumination, depending on their shape and material composition, and will not protect the bulb from paint. Above-ground power supplies are vulnerable to tampering, while underground utilities are vulnerable to corrosion from the soil surrounding the conduit, flooding, and excavation accidents, as well as such lines being more expensive to replace.

TRENDS

Jenkins and Claire note that as the ISIS effort failed in Syria, a number of former ISIS fighters have returned to their homes in Europe. Some are determined to bring the war to Europe. A pre-existing criminal class in Europe combined with these returning adherents of a terrorist ideology to create a network of terrorists. They carried out multi-faceted attacks in Paris on November 13, 2015 that left 130 people dead from explosions, shootings and suicide vest detonations. In Belgium on March 22, 2016 another 35 people were killed in two transportation-related explosions: the airport and a metro station. The French government believes that these attacks were controlled by ISIS from Syria, but that that network has now been disbanded.[100] The lesson learned by the next ISIS fighter

generation may be to go it alone.

Lone wolf vehicle attacks have risen in frequency because they are simple. They do not require coordination among conspirators, varied skills or wide knowledge in order to be carried out. The Rand Corporation's report *Aptitude for Destruction* notes that more sophisticated attacks lead to complexity, and the challenge of operational security rises with the number of people involved in an operation.[101] There is also a higher likelihood of observers recognizing that something unusual is happening when there are multiple actors, and when there is a need to acquire noticeable resources (e.g., two end caps and a short piece of pipe, hinting that a pipe bomb may be built).

Also, as conspirators try to develop the attack they may ask questions that, taken together become suspicious. These questions may form a pattern that reveals actions to the FBI. This possibility for observation makes a lone wolf model desirable to the attacker. Militia movements and eco-terrorists of the 1990s have favored lone wolf tactics because they are easier to use covertly, as described in *Eco Defense*.[102]

In America, most people have access to a vehicle. Most people know how to drive, or can learn without attracting suspicion. Terrorists are shifting to simple methods– lone-wolf vehicle attacks - because complex approaches are easier to detect and disrupt. This approach enables a single person to engage in terrorist acts like the Nice and New York vehicle-ramming attacks that generated worldwide attention.[103] The ease with which lone-wolf vehicle attacks can be replicated by a single individual with little skill also makes the attacks psychologically disturbing. Bomb building, or even the skilled use of a rifle for mass killing, requires concerted effort and unique resources; in contrast, most people drive a car, accidents occur every day, and the possibility of intentionally running over people does not require any imagination.

First responder knowledge about terrorist tactics has been lost since 9/11. Rotation of personnel to new positions, attrition in the ranks of law enforcement, and retirements among first responders have all resulted in loss of first-hand knowledge gained through training delivered after terrorist events. While some focused counter-terrorism training has continued, less emphasis is placed on terrorism preparedness, while scarce resources have been redirected to other operational needs, like active shooter and civil unrest. Right after the Oklahoma City bombing and sarin attack in Tokyo in 1995, Metropolitan Medical Task Forces (MMTF) were created in 27 American cities in 1996,[104] with a significant contribution in first responder personnel time by the local jurisdictions. For example, in one-year San Jose Police Department spent $1 million in overtime to train their officers in responding to attacks with weapons of mass disruption, such as dirty bombs or anthrax attacks.[105] After 9/11, the MMTF program was transitioned to the Metropolitan Medical Response System (MMRS), an approach focused less on public safety responders and more on medical personnel. The anthrax attacks which followed 9/11, and the threat of infectious disease outbreaks like Ebola and pandemic flu, have changed the focus from public safety responders to medical response. The knowledge developed in the earlier MMTF training and exercise programs has atrophied or been lost altogether through retirements, promotions and job position rotations. Today's public safety personnel have never received the weapons of mass disruption field response training.

Similar losses of practical knowledge have happened before. In World War II, military personnel were trained on railroad derailing, how to damage trains, and on booby-trapping. Again, in the Vietnam War sabotage training was offered and used by troops in the field. Military personnel recognized that if it is self-propelled it can be made to be self-destructive.[106] A focus on all hazards can blend with the specific hazard of chemical, biological, radiological, nuclear and explosive (CBRNE) training to enhance public safety first responder capabilities. Training for responding to chemical attacks can also apply to response to pipeline accidents or other accidental releases of hazardous materials. Preparation for biological attacks applies to managing an outbreak of pandemic flu. Response to a terrorist's bomb is similar to response to an explosion in an ANFO plant or refinery.

Recently, with the advent of vehicle ramming strategies and the resurgence of explosives attacks, law enforcement has heightened its focus on terrorism threats. Effective intelligence gathering, and infiltration and disruption of terrorist groups by law enforcement, have forced terrorists to use simpler attack methods, such as lone wolf vehicle ramming attacks. This is a prime indicator that the systems for interdiction of terrorist acts by law enforcement are working against cell-oriented strategies. It remains to be seen whether they will be effective against the single actor. It reinforces the need to maintain training on all forms of potential terrorist activity to be prepared for evolving terrorist strategies.

V. CASE STUDIES: ORDINARY EVENTS CAN BECOME TERRORIST BLUEPRINTS

BALTIMORE TUNNEL FIRE

Scenario

On July 18, 2001 a CSX freight train of 60 cars was traveling through the city of Baltimore using the Howard Street tunnel, the only rail access through the city. The train was carrying a combination of 31 loaded and 29 empty cars. The loaded cars were behind the empty cars, which is known to cause bumping and derailments. The loaded cars' cargo included hazardous materials such as hydrochloric acid and tripropylene, as well as other goods including pulp board, wood pulp, brick, soy oil, paper, plywood, and steel. At 3:04 pm as the train was 1000 yards into the tunnel through its south entrance, traveling at 23 mph, 11 cars derailed, including 4 of the cars carrying hazardous materials. A fire started from unknown sources, igniting the wood and paper. Due to the derailment, and the damage to the cars that it caused, 2,554 gallons of hydrochloric acid were released. The emergency brake was engaged and the crew dismounted to investigate.[107]

At 3:27 pm the crew disengaged the engine and proceeded to exit the tunnel from the north end, and contacted their dispatcher. At 4:00 pm the Baltimore Fire Department received the first notification of the derailment from CSX. At about the same time there were reports of smoke coming from manholes along Howard Street in downtown Baltimore. At 4:10 pm the fire crew arrived at the North Portal to connect with the train crew and establish the Incident Command Post, and learned of the hazardous materials spill. By 4:30 pm all the roads into the city were closed. The initial Incident Action Plan priorities were 1) to assess the train and its contents; 2) to attack the fire, and 3) to protect the community. At 4:45 pm a shelter-in-place order was issued for residents, and the Orioles' ballpark, Camden Yards, was evacuated and the baseball game was cancelled. The Baltimore Fire Department had committed five alarms (fire engines, fire trucks and battalion chiefs) to the event by 5:30 pm. At 5:45 pm the civil defense siren sounded. The temperature inside the tunnel reached 1,500 degrees.

The tunnel is made of 30 million bricks, and is over 100 years old. It runs under Howard Street, a main shopping street in downtown Baltimore. Above the tunnel on the surface is the light rail line. At its deepest point the tunnel is 49 feet below ground, and it is 27 feet wide. There is only one access point aside from the ends, a manhole at Howard and Lombard Streets leading to a gallery inside the tunnel. The north end of the tunnel opens into a commercial and residential area that includes Maryland General Hospital. The south portal is near Camden Yards and M&T Bank Stadium. The whole area is densely populated.

At 6:15 pm the water main at Howard and Lombard Streets collapsed, flooding streets and nearby buildings, and pouring water into the tunnel. This accident helped to dilute the acid and put out the fire. The storm drains empty into the Inner Harbor, so the US Environmental Protection Agency and Coast Guard responded to monitor the run off. When contaminants were discovered in the Inner Harbor, booms were placed to contain them.

By 9:00 pm roads into the city began to reopen. By 11 pm the water flow was cut off to the pipe break. By July 20 fire suppression was largely completed. Cars were then removed from both ends and the smoldering wood and paper extinguished. Fire crews used a vacuum truck with a hose down the manhole to remove the remaining hydrochloric acid from the damaged tanker car.[108]

On July 23 the last train car was removed from the tunnel, and by July 24 the tunnel was again in rail use. Water main repairs were completed July 29. On August 11 chemicals left in a storm drain ignited and blew off manhole covers near the derailment site.

Impacts on Baltimore were notable. Major sections of the downtown area were closed for three days. Cancellation and rescheduling of the double-header baseball game cost over $4.5[109] million in losses. Portions of Howard Street were closed for 5 weeks while repairs were made to the broken pipe and to light rail tracks that had been twisted by the heat. The conduit for fiber optic cable had run down Howard Street, and it was destroyed by the heat, a loss which affected communications as far away as Africa. To achieve immediate service restoration a new fiber optic line was laid a few blocks east of Howard Street. Crew laid 30,000 feet of fiber optic cable in two days.

Transportation impacts affected the whole eastern seaboard. Two interstates were closed for a short time on July 18. Most local streets in Baltimore's downtown were closed for five days, with some being closed for up to seven weeks. The light rail lines were severed where the street collapsed at the pipeline break. Repairs and testing took 53 days. The tunnel is the main north/south route for CSX, and there was no rail service through it for 5 days. Some north/south trains were held at origin, and others were re-routed for hundreds of miles in order to get around the damaged tunnel, going as far west as Pittsburgh. There was no closer alternate route between Florida and New York.

The National Transportation Safety Board (NTSB) issued their report on the accident in December 2004, and it was inconclusive. The source of the ignition was never conclusively determined because all the evidence was destroyed by the 1,500-degree fire and the deluge of water. There was no loss of life and no serious injury. The Incident Command System provided coordination among local, state and federal agencies who partnered to resolve the event. CSX was considered to be the responsible party, and ultimately reimbursed the city for response costs and water main and light rail damage.[110]

Lessons Learned

Lessons learned from this accident included the need for more thorough disaster planning; the city and CSX had never made a disaster plan for the tunnel. Private sector cooperation went well. The US Fore Administration regarded the management of the event as a classic example of highly successful ICS implementation with multi-agency involvement. The study and evaluation of the entire event was over-shadowed by the 9/11 attacks on the Pentagon and World Trade Center that occurred just a few weeks later. For example, it took three years for the US Fire Administration to issue its report on the fire.

This event was an accident of unknown origin. An intentional attack using the same modality

and in the same location could have been much worse, including the possible spillage of additional hazardous materials that could have generated lethal smoke in the downtown area. It provides a planning paradigm of a cascading disaster: fire and flooding leading to loss of transportation and loss of communication.

SAN JOSE TRANSIT MALL COLLAPSE

Scenario

On Columbus Day in 1992 the San Jose Water Company decided to pressure test their pipes running through the downtown of San Jose. They did not notify the city, as it was a holiday weekend when the Public Works department was closed, and the testing was all underground. At 10 am the Police 9-1-1 center received a call that the newly constructed transit mall on San Carlos Street between 2nd and 3rd Streets had collapsed. The dispatcher notified the fire dispatch center, who called the first due fire company and the city's director of emergency preparedness (DEP).

By 10:30 am the fire department's damage assessment revealed that the center of the street had collapsed, destroying the newly laid light rail tracks. The phone lines were visible, suspended above the gaping hole. There was water running in the gutters with rainbow-colored liquid floating on the top, an indicator of the presence of a petroleum product. The gutters ran into a storm drain system that flows to Coyote Creek and then to the lower San Francisco Bay, an ecologically sensitive area with endangered species resident, including the salt marsh harvest mouse. The fire department's hazardous materials team installed petroleum absorbing booms as soon as they arrived at the scene, but hundreds of gallons of water had already escaped to the creek before they were called out, since the initial report had only been of a street collapse, not a hazardous materials event.[111]

By 11 am it was determined that the source of the water was a pipe in the street, which proved to belong to the privately-owned San Jose Water Company. The DEP called the water company, who said that they noticed that their water pressure had dropped and were trying to understand why. They agreed to shut off the water and send a repair crew immediately.

Further investigation revealed that the San Jose Title Company at the corner of 2nd and San Carlos Streets had a basement that was filled with paper records of deeds and titles, and also housed the furnace for the building. Although the heating was now run on natural gas, the original system had run on fuel oil, and the old tank had been left in the basement with the residual fuel oil still in it. As the basement filled with water, the flood had entered the old fuel tank and the oil floated out, up and into the street as the water rose.

The broken water pipe had flooded the new transit mall underground from curb to curb and pushed out all the sand and gravel engineered fill on which the asphalt had been laid. Beneath the surface were gas lines, which were undamaged; electrical lines in sealed conduit; and the dangling phone lines, which continued to work. For safety, all the utility lines that ran under the collapsed street were de-energized or shut down, denying the residential and commercial neighborhood any services for several blocks.[112] San Jose

State University was just one block east. Monday classes were in session, as Columbus Day is not a university holiday, and so disruptions resulted when classrooms, dining facilities, offices and dormitories that shared the electrical circuit were also affected. The street was closed for repairs for three months, well into the rainy season.

Lawsuits dragged on for years, as the water company tried to blame the new transit mall construction for damage to its pipes, but the courts determined that the damage was caused by the excessive water pressure used in the test. The title company, which belonged to the congressman's ex-wife, suffered the most damage, and moved away from that area of town.

Lessons Learned

Lessons learned from this event included the need for better coordination between the water utilities and the city's public works department, and public safety agencies. It also demonstrated the importance of the San Jose Fire Department's hazardous materials team in providing a rapid response to the appearance of an unknown substance in the community—the "rainbows" on the water. Having emergency contact numbers for the water utility was critical in the relatively quick resolution of the flooding, demonstrating the importance of regular updating of all emergency contact numbers for critical infrastructure owners and key emergency response partners. In the past the water companies' operations had been viewed by the city mainly as fire department emergency response services that could enhance water pressure to hydrants in the event of a large fire. However, this event demonstrated that utilities could also be the cause of a problem, or the victim of a system failure.

The over-pressurizing of the water pipe in this instance was an operations failure of the private water retailer. It demonstrated, however, that an intentional over-pressurizing of water pipes could also potentially cause infrastructure collapse. If intentionally organized by terrorists on a normal business day, there would have been pedestrians, and bus, light rail and car traffic on the street when it collapsed, hemmed in by the sidewalks and median, falling into the hole. Hazardous materials could have been introduced into the scene, along with snipers in the surrounding high rise buildings to impede emergency response. Air borne hazardous materials could have necessitated the evacuation or shelter-in-place of 10,000 or more students from the SJSU campus.

GILROY AT&T DENIAL OF SERVICE SABOTAGE

Scenario

Fiber optic cable carrying internet, land line and cell phone services in the southern part of San Jose, California was deliberately severed by saboteurs at 1:30 am on Thursday, April 9, 2009. The saboteurs climbed into a manhole at Blossom Hill Highway and Monterey Road and severed the fusion splicer, 8 feet underground. The fiber optic cables served Morgan Hill and Gilroy, two communities in south Santa Clara County. The result was a loss of phone, cell and internet service, causing the loss of 9-1-1 services, as well as all normal phone service in parts of south Santa Clara County, San Benito County and Santa

Cruz County. AT&T repair crews had to check each manhole in person to find the damage, which also included cuts at two other south San Jose manholes that affected three San Jose neighborhoods.[113]

At about the same time, AT&T lines were cut at Britton and Industrial in San Carlos, causing phone service outages in San Mateo County. While no disruption of service resulted from the sabotage at this location, the damage at the four sites was considered a coordinated denial of service attack by the law enforcement community.[114]

In Gilroy and Morgan Hill 52,000 customers lost service, including hospitals and the 9-1-1 centers. Amateur radio operators (Radio Amateurs in Civil Emergency Services – RACES) were called out to provide alternate emergency communications throughout the communities. They set up communications stations at key intersections in the community with magnetic signs identifying themselves to the community as emergency contact points. RACES also served the hospitals, fire stations, the cities' emergency operations centers and the public safety answering points (PSAPs) to ensure that emergency responses could continue. Mutual aid from the Santa Clara County Sheriff's Department, the California Department of Forestry and Fire Protection, and the San Jose Police Department extended the emergency response capabilities within the community. Fire equipment was staged throughout the community, while one firefighter/paramedic was kept at each fire station in case community members went there for assistance.

The business community was also impacted, because alarm systems, credit card readers, automatic teller machines (ATMs) and check verification systems are all dependent on phone lines or internet connections. Banks only allowed one client at a time into the lobby, the only way to get any banking service. Gas stations required exact change because credit cards readers at the pumps did not work. Businesses began requiring cash-only transactions, inconveniencing customers and reducing sales, resulting in significant lost business for April 9.

Cisco Systems donated the services of its network emergency response vehicle (NERV). The truck-mounted satellite dish provided phone internet conferencing and Wi-Fi for the Morgan Hill EOC within 30 minutes of its arrival. While useful for that EOC, it only met a small part of the emergency operation's needs. Satellite phones were useful, but being priced at $1,000 per year for connectivity these were not widely used.

Lessons Learned

Emergency response and callback activities had come to rely on phone and internet contact information. The city manager had recently moved to a new home, and it was discovered that no one in the PSAP or on duty in public safety had his new address. When they were able to contact the Personnel Department staff at home and get the city manager's address, they discovered that the cul de sac where he had moved had no house numbers, so they woke up several neighbors before finding the city manager. This reinforced the importance of having current physical addresses for all key city staff, and for having all inhabited houses clearly marked with an address number.

Within Santa Clara County there is an EOC-to-EOC commercial radio system that continued working during the outage. However, it was not included in the Morgan Hill EOC operations plan, so no one was assigned to answer the radio, meaning that contacts from the county's EOC did not get through. The PSAP dispatchers said that they were too busy to answer the extra radio. This meant that countywide mutual aid and other assistance was delayed while the county EOC staff had to find other sources of situation intelligence until the RACES volunteers delivered the first situation status report as a packet radio message to the county EOC's RACES station.[115] The importance of communications redundancy and thorough staff planning for critical communications positions was demonstrated.

The American Red Cross had its emergency communications vehicle, which is normally located in Sacramento, in Santa Clara County instead. The vehicle had $750,000 in satellite and connectivity equipment, but new operators. It took them four hours to establish the satellite link, because it is shared with Disney and they had to contact their Washington, DC headquarters to ensure that their emergency response would not interfere with Disney's needs. They then needed power for the unit, and rather than use their generator, since regular power was available, they plugged into available power in the City of Morgan Hill building, which meant that they propped open the door to the EOC, compromising their security.

Verizon had previously given an orientation to law and fire leaders about their emergency communications towers, which could be deployed to provide communications, such as after an earthquake. The fire chief of Gilroy requested the deployment of the towers for this event; however, the Verizon representative at the county EOC said that they could not use that system for communications because it requires a hardline connection into the AT&T system, which is what had been cut, and so the towers were useless. This demonstrates the importance of getting complete documentation for all work-arounds and emergency systems that an agency plans on using. Before including an asset in the emergency plan, all of its requirements and limitations should be documented.

The most crucial lesson from this sabotage event was the vulnerability of the communications infrastructure, and the impact of its loss across the community and economy. The amateur radio operators urged all public safety agencies to hold regular drills of all communications assets to ensure that systems work as expected, and that adequate information and trained staff are available to run them.[116]

While this sabotage appeared to be the work of a disgruntled individual, it could have been a dry run by terrorists. Even with a $250,000 reward offered, no perpetrator has ever been arrested. It would have been possible for terrorists to take advantage of the lack of public safety communication and coordination, caused by the loss of the PSAP, to commit other crimes, facilitated also by the loss of alarm systems. Burglaries for supplies, resources and materials, illegal entries to plant explosives, kidnapping of high-profile executives and their families would all have been possible once the communications network was disabled. The sabotage clearly demonstrated the connectivity and vulnerability that could have become the basis for a more destructive plan.

NYC VEHICLE RAMMING EVENT, 2017

Scenario

Halloween 2017 was selected by ISIS affiliates for terror attacks. In their magazine, *Rumiyah*, ISIS exhorted their followers worldwide to "mow down pedestrians with trucks, continue the attacks with a knife or a gun and claim responsibility by shouting or leaving leaflets."[117] A French pro-ISIS group added the specific threat for Halloween. Sayfullo Saipov, a green card holder living in Paterson, New Jersey, rented a pick-up truck at Home Depot in Passaic, New Jersey, a town near Paterson, and drove to New York City. He rented the truck at 2:06 pm, and by 3:04 pm had entered a fenced-off, restricted access bike path at Houston Street. He drove south on the path for five blocks, killing six at the scene, and fatally injuring two others. Eleven others were injured non-fatally. Those dead at the scene were tourists, five from Argentina and one from Belgium. The pick-up truck stopped when it crashed into a school bus at Chambers and West streets near the World Trade Center site, injuring two adults and two children on the bus.

Saipov exited the crashed truck with a pellet gun in one hand and a paint ball gun in the other, shouting in Arabic. He had left handwritten notes scattered around the truck declaring his allegiance to ISIS. He was from Uzbekistan, and had lived in Florida. Aside from his attack and note there was nothing linking him to ISIS or other terrorist groups.[118] He was able to enter the bike way through an opening intended for city vehicles to use to maintain the pathway or provide medical assistance to those using the Hudson River Bike Path. He killed three near the entrance at Pier 40, three just before Laight Street, and two next to the Stuyvesant High School.

Before he could shoot anyone with either the pellet gun or the paintball gun, Saipov was shot by a police officer, but survived. Because this was a terrorist attack, the case is currently being prosecuted by the federal government. He has been charged with eight counts of murder, 18 counts of attempted murder, and terrorism charges. His lawyers are contending that the government had him under surveillance for three years, evidence from which may reveal that he was radicalized by his associates, making them partially responsible for the bike path rampage, and thereby sparing his life. His trial is set for April, 2020.[119] In a June 2018 court appearance, Saipov testified that ISIS is "fighting to impose Sharia law on earth."[120]

Lessons Learned

Bike paths are intended to protect bike riders from motor vehicles by creating a separated area. However, when a truck intentionally violates the traffic laws and enters the restricted area, the separation also makes it more difficult for police units to access the area to protect the potential victims and interdict the terrorist act. The lesson learned from this terrorist attack is that the emergency entrances to the bike path must be blocked by sturdy barriers that can only be removed by authorized city vehicles. Some cities use bollards that are padlocked to ground-level sleeves, while others use gates that can only be raised by an encoded or infrared system like the emergency vehicle preemption systems used by public safety to change traffic lights. The goal is a system that prevents intruders while

facilitating the rapid access of public safety vehicles. A physical barrier is the only reliable method for stopping pedestrian ramming by motor vehicles.

This situation might have been worse if individuals had not been alert to their environment. The screams and shouts of others and the sounds of the vehicle allowed some potential victims to become aware of the hazard and take protective actions. The eleven injured survivors were reported by observers to have diverted their paths, jumped off their bikes or tried to jump over the rail. Thus, situational awareness can contribute to personal safety, even in a concerted attack.

The Department of Homeland Security has distributed a document titled "Vehicle Ramming –Security Awareness for Soft Targets and Crowded Places," which provides guidance on securing public gatherings against terrorist activity. They advise that "The use of vehicles as weapons often has few or no observable indicators but identifying and reporting suspicious activities may assist in detecting a potential vehicle ramming attack plot."[121] A list of potential indicators of ramming attacks is provided in the document. Physical security and thorough planning of large events can provide deterrence. Ultimately, there is no way to completely protect large groups of people from a determined attacker, but barriers and well developed plans may harden the target sufficiently to turn the would-be attacker to a different location, which may in turn be easier to protect.

VI. CONCLUSION

VALUE OF COST/BENEFIT THINKING

While terrorist attacks gain wide media coverage it is because they are rare. Jenkins and Butterworth's 2018 study of vehicle ramming[122] showed a stark contrast between "normal" accidents and terrorist attacks, writing that "in the United States alone, approximately 6,000 pedestrians are killed by vehicles annually. In contrast, car-ramming attacks have killed 300 people since 1973."[123] Therefore, it is important to consider what benefit is being purchased at what cost through counterterrorism efforts. While it is tempting to buy sophisticated technology, it is important to ask what the initial and long-term costs will be, and whether the outcomes for the pedestrians and users of the facility will in fact be better after its installation. In some cases, cutting corners by installing "dummy cameras" or other decoy systems instead of real cameras may actually cause harm, as in the BART example.[124]

Pedestrian education can be a simple and inexpensive approach with immediate benefit. Campaigns to urge situational awareness, discourage jay-walking, and remind people to avoid going into dark spaces alone at night can have a significant beneficial effect on crime rates and victimization. Researchers note that it can take between eight and twelve years to change pedestrian behavior, yet the Street Smarts campaign to stop pedestrian deaths noted a reduction in unsafe pedestrian behavior after one year.[125]

Better lighting, cameras and fences can all contribute to deterring vehicle ramming and other terrorist attacks on pedestrians and transit facilities. Judicious use of technology can deter criminal and terrorist acts by enhancing the likelihood that they will be stopped before completing their mission. Intermittent use of enhanced patrol, bomb sniffing dogs, and VIPR teams can add a layer of uncertainty that may in itself be a deterrent. Rapid response to reports of suspicious vehicles, inappropriate driving or vehicles where they do not belong can interdict or discourage attacks that are attempted. If a terrorist goes on a surveillance run and is interviewed by law enforcement about his presence and purpose, that may suggest a hardened target that he will avoid.

Physical barriers need not be ugly or expensive. Trees and planters along the street edge can protect pedestrians from intentional or accidental intrusion of vehicles onto the sidewalk, while also adding charm to the urban environment. Temporary activities like markets and festivals can be protected by parking recycling trucks across the perimeter streets to block access.[126] While a car or pick-up truck might be moved out of the way by ramming, a recycling truck is very difficult to displace by another vehicle.

VALUING DUAL USE DETERRENCE

Investing in new infrastructure can be more easily justified when it will serve two or more purposes. Transit center parking lots can be havens for crime at night. Installation of cameras, fencing and improved lighting might deter rapes, car burglaries and muggings, as well as terrorist attacks and vehicle ramming. A drop in the violent crime and property crime rates would have an immediate beneficial economic value, while deterring potential

terrorism against the transit infrastructure would have long-term benefit.

Streetscapes, and the creation of separated pedestrian walkways and bike paths, can enhance quality of life in urban settings while also protecting vulnerable pedestrians and riders against vehicle ramming, whether accidental or intentional. The rising number of elderly drivers who mistake the gas pedal for the brake,[127] and the proliferation of cell phone-related pedestrian accidents,[128] both contribute to a rise in vehicle-pedestrian collisions. Some fault often lies with the inattentive pedestrian; for example, texting while walking is known to be dangerous. Providing physical separation at-grade, and pedestrian and bike road and rail overcrossings, however, can prevent accidents, while also deterring vehicle ramming.

Inevitably, public works vehicles and emergency vehicles must have access to pedestrian walkways and to bikeways for maintenance, cleaning, landscaping and medical emergency (EMS) response. Their access points should be guarded with devices that require the use of a vehicle limited access automated system for EMS, or an electronic gate code for access to other vehicles with a legitimate purpose for entering the limited access area. The tragic ramming on the New York City bikeway in 2017 demonstrated the danger of leaving readily accessible gateways. Access for bikes and pedestrians should be as narrow as possible—for accessibility's sake, one wheelchair wide. Twin strollers and other larger vehicles would have to be lifted over the entrance point, no doubt annoying some users, but defending against small cars and large motorcycles that could readily cause fatal events. Access points guarded by removable bollards with combination locks have been tried, but a terrorist can get a combination from a public agency as easily as can a mother with a stroller.

FOCUS ON SAFETY

Jenkins and Butterworth note that the best investments to deter ramming are those that also enhance safety against accidents, since 6,000 pedestrians are killed in accidents in the United States alone every year, and many more are injured.[129] Pedestrian education campaigns and heightened enforcement of jay-walking and cell phone usage laws might improve pedestrian safety. Greater situational awareness by pedestrians would also alert them sooner to potential ramming, possibly allowing for self-protective measures as suggested by DHS, such as moving away from the vehicle at a right angle or sheltering behind a tree or other barrier.[130] Trees and planters, bollards and entry ways, cameras, fences and lighting can all contribute to enhanced safety against accidents, while also deterring ramming on public streets and in public places. Attack mitigation, like rapid medical response, is possible, but prevention requires the cooperation of the public, streetscape designers and law enforcement personnel, using the lessons learned about safety and security through the years.

GLOSSARY

Alarm	In the fire service, a specific group of resources that are dispatched to the emergency. For example, an alarm may be defined as two fire engines, one fire truck and one battalion chief.
Deny access	Create a barrier that keeps someone out of an area
Detect	Recognize that someone is in an area
Deter	Create activities that make entry, or carrying out an activity, unlikely, or less likely to be successful, such as “guard dogs would deter most people from jumping the fence.”
Due	In the fire service, a term for the order in which fire service resources will be sent to an emergency, such as “the first due engine is three minutes away.”
Emergency Operations Center (EOC)	The place from which an emergency is managed; may be at city, county, region, state or national levels.
Incident Command System (ICS)	A method for organizing and tactically managing resources for response to an emergency that uses five functions: command, operations, planning/intelligence, logistics and finance/ administration. By law ICS is the basis for all multi-jurisdiction emergency response in the United States.
Intercept	To cut someone or something off from its intended destination, such as “the coded message was intercepted by the NSA.”
Interdict	To intercept and stop the movement of a person or commodity, such as “the police set up roadblocks to interdict the drugs.”
Mitigate	Lessen the impact of an unwanted action that cannot be stopped, such as, “the levees mitigated the flooding in the neighborhood.”
National Incident Management System (NIMS)	A method for organizing and strategically managing resources for response to an emergency that uses ICS in the field, and parallel methods inside the EOC or other emergency response structure; preparedness, mitigation and command and control; required for all multi-jurisdictional emergency response in the United States.
Packet radio	A digital radio communications system used by amateur radio operators to send messages as data instead of voice.
Prevent	To stop something from happening
Resilience	To recover quickly from an unwanted event or emergency, to “bounce back”

Safety	Being protected from damage, risk or injury; usually refers to an accidental or unintentional cause; usually refers to human beings and their interaction with the built environment or machinery, such as “passengers are required to wear seat belts for their safety,” but may include the protection of goods.
Security	Methods to project an asset from criminal or intentional damage or disturbance; usually refers to physical structures or goods, such as “the security system includes alarms to deter burglaries,” but may also apply to people.
Staging Area	In the fire service, a designated location where resources and personnel are stored until they are needed at the scene of an event.
Streetscape	The elements that create the visual appearance of a street, such as landscaping, road surface material and color, signage, lighting, building facades, street furniture and open spaces.
Transportation Security Agency (TSA)	The agency within the US Department of Homeland Security that focuses on transportation modes. While best known for its work in airport passenger screening, TSA is responsible for enhancing the security of all seven identified modes of critical transportation.
Visible Intermodal Prevention and Response (VIPR)	Mixed teams of law enforcement agents from a variety of federal services who conduct random searches of travelers in stations, rest stops, platforms, terminals and other transportation-related locations. They are looking for contraband, weapons, IEDs and other harmful materials that could put passenger and mode safety and security at risk.
Weapons of mass destruction	Weapons that are capable of widespread destruction, usully referring to nuclear devices; or to chemical, biological, or explosive devices designed to kill large numbers of people, and destroy the built and natural environments.
Weapons of mass disruption	Weapons that are aimed at causing social and economic damage without causing large loss of life or property destruction, for example, a radiological “dirty bomb” that would kill few people but would take time and be expensive to clean up, or a cyber attack on an electric grid.

ENDNOTES

1. Intelligence is defined as information that has been investigated and confirmed.

2. Brian Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed May 3, 2019).

3. Mike Davis. Buda's Wagon: A Brief History of the Car Bomb. (New York: Verso, 2007).

4. Albert Lulushi. Donovan's Devils: OSS Commandos Behind Enemy Lines- Europe, World War II. (New York: Arcade Publishing, 2018).

5. Brian M. Jenkins and Frances L. Edwards-Winslow. Saving City Lifelines. (San Jose, CA: Mineta Transportation Institute, 2002), http://transweb.sjsu.edu/research/saving-city-lifelines-lessons-learned-9-11-terrorist-attacks (accessed July 15, 2018); Brian M. Jenkins. Protecting Public Surface Transportation against Terrorism and Serious Crime: Continuing Research on Best Security Practices. Report 01-07. (San Jose, CA: Mineta Transportation Institute, 2001). http://transweb.sjsu.edu/MTIportal/research/publications/summary/0107.html (accessed July 15, 2018).

6. Brian M. Jenkins and Frances L. Edwards-Winslow. Saving City Lifelines. (San Jose, CA: Mineta Transportation Institute, 2002), http://transweb.sjsu.edu/research/saving-city-lifelines-lessons-learned-9-11-terrorist-attacks (accessed July 15, 2018); Fernando Reinares. Al-Quaeda's Revenge: The 2004 Madrid Train Bombings. (New York: Woodrow Wilson Center Press, Columbia University Press. 2017); Hamilton Bean, Lisa Keränen, and Margaret Durfy. "This is London: Cosmopolitan Nationalism and the Discourse of Resilience in the Case of the 7/7 Terrorist Attacks." Rhetoric and Public Affairs, vol. 14, no. 3, 2011, pp. 427–464; Jill Lawless. "Surveillance in the U.K. 'just kept expanding' after the London bombings". Business Insider. 2015. http://www.businessinsider.com/surveillance-in-the-uk-just-kept-expanding-after-the-london-bombings-2015-7 (accessed July 1, 2018).

7. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

8. BBC News. "London attack: police know Identities of killers." June 5, 2017. https://www.bbc.co.uk/news/uk-40155451 (accessed June 5, 1018).

9. Gemma Mullin. "Terror Atrocity: What Happened in The 7/7 London Bombings, How Many Victims Were There in the Terror Attack and Who Were the Bombers?" The Sun. July 7, 2017. https://www.thesun.co.uk/news/3966186/july-7-london-bombings-victims-terror-attack-bombers/ (accessed July 1, 2018).

10. Jill Lawless. "Surveillance in the U.K. 'just kept expanding' after the London bombings". Business Insider. 2015. http://www.businessinsider.com/surveillance-in-the-uk-just-

kept-expanding-after-the-london-bombings-2015-7 (accessed July 1, 2018).

11. American Civil Liberties Union (ACLU). “Surveillance cameras and the attempted London attack”. 2018. https://www.aclu.org/other/surveillance-cameras-and-attempted-london-attacks (accessed June 5, 2018).

12. American Civil Liberties Union (ACLU). “Surveillance cameras and the attempted London attack”. 2018. https://www.aclu.org/other/surveillance-cameras-and-attempted-london-attacks (accessed June 5, 2018).

13. IFSEC Global. “Role of CCTV Cameras: Public, Privacy and Protection.” January 1, 2014. https://www.ifsecglobal.com/role-cctv-cameras-public-privacy-protection/ (accessed June 14, 2018).

14. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

15. Annie Palmer. “AI surveillance cameras would soon identify faces in a crowd with 99 percent accuracy.” Daily Mail. February 16, 2018. http://www.dailymail.co.uk/sciencetech/article-5401325/CCTV-cameras-soon-face-recognition-technology.html (accessed June 14, 2018).

16. Brian M. Jenkins. The Challenge of Protecting Transit and Passenger Rail: Understanding How Security Works Against Terrorism. (San Jose, CA: Mineta Transportation Institute, 2017). http://transweb.sjsu.edu/research/challenge-protecting-transit-and-passenger-rail-understanding-how-security-works-against (accessed July 15, 2018).

17. Department of Justice (DOJ). Report on the Availability of Bomb Making Information. (Washington, DC: US Department of Justice, 1997).

18. Department of the Army. Boobytrapping, FM 531. (Washington, DC: Department of the Army, 1965).

19. Department of the Army. Unconventional Warfare Devices and Techniques: Technical Manual 31-200-1. (Washington, DC: Department of the Army, 1963).

20. Department of the Army. Improvised Munitions Handbook. Technical Manual 31-210. (Washington, DC: Department of the Army, 1969).

21. Dupont, E.I. de Nemours. Blaster’s Manual. (Wilmington, De: Dupont & Company, Incorporated, 1922). https://the-eye.eu/public/Books/campdivision.com/Sensitive/Anarchy%20Folder/Explosives%20%26%20Incendiaries/Demolition%2C%20Blasting%2C%20Sabotage/Dupont%20Blasters%20Handbook%201922%20ed.pdf (accessed July 1, 2019); Dupont. Blaster’s Manual, 15th edition. (Wilmington, DE: Dupont Sales Development Division, 1969).

22. J.M. Berger. “How Terrorists Recruit Online and How to Stop It”. (Washington,

DC: Brookings Institution, November 9, 2015). https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/ (accessed June 12, 2018); UN Office on Drugs and Crime. The Use of the Internet for Terrorist Purposes. (New York, NY: United Nations, November, 2012). https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed June 15, 2018).

23. UN Office on Drugs and Crime. The Use of the Internet for Terrorist Purposes. (New York, NY: United Nations, November, 2012). https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed June 15, 2018).

24. Union Pacific. “Positive Train Control.” https://www.up.com/media/media_kit/ptc/about-ptc/ (accessed July 2, 2019).

25. Seattle Times Staff. 4 dead, 2 critically injured in collision between Ride the Ducks vehicle, charter bus on Aurora Bridge. Seattle Times, September 24, 2015. https://www.seattletimes.com/seattle-news/ride-the-ducks-vehicle-collides-with-bus-on-aurora-bridge/ (accessed June 12, 2018).

26. CBS News. “4 remain critical after tour bus crash in San Francisco”. CBS News. November 15, 2015. https://www.cbsnews.com/news/4-remain-in-critical-condition-after-tour-bus-crash-in-san-francisco/ (accessed June 14, 2018).

27. Associated Press. “Eight remain hospitalized after San Francisco Tour Bus Crash.” The Guardian. November 14, 2015. https://www.theguardian.com/us-news/2015/nov/14/san-francisco-double-decker-tour-bus-crash (accessed June 30, 2018).

28. Michael Cabanatuan and Kale Williams. “Driver blamed for tour bus crash in SF’s Union Square”. SF Gate. March 23, 2016. https://www.sfgate.com/bayarea/article/Driver-blamed-for-tour-bus-crash-in-SF-s-Union-6994435.php (accessed June 30, 2018).

29. Jeff Horwitz. “Who’s at fault in Amtrak Crash?” Associated Press/ Miami Herald, February 10, 2018. https://www.chicagotribune.com/nation-world/ct-amtrak-crash-payment-agreements-20180210-story.html (accessed June 13, 2018).

30. Alan Blinder, Christina Caron, and John Jeter. “Fatal Amtrak Crash in South Carolina Is New Challenge for Rail Service”. The New York Times. February 4, 2018. https://www.nytimes.com/2018/02/04/us/amtrak-crash-south-carolina.html (accessed July 2, 2018).

31. Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways. (Oakland, CA: Battelle Memorial Institute, 2018), p. 4.

32. Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways. (Oakland, CA: Battelle Memorial Institute, 2018).

33. Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways.

(Oakland, CA: Battelle Memorial Institute, 2018), p. 7.

34. Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways. (Oakland, CA: Battelle Memorial Institute, 2018).

35. Madison Park and Holly Yan. "What is Positive Train Control, and could it have prevented the Amtrak crash?" CNN. February 5, 2018. https://www.cnn.com/2018/02/05/us/positive-train-control-explainer/index.html (accessed July 12, 2018).

36. Kim Zetter. "An unprecedented look at Stuxnet, the world's first digital weapon." Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed June 30, 2018).

37. Swati Khandelwal. Dangerous malware discovered that can take down electric power grids. Hacker News. June 12, 2017. https://thehackernews.com/2017/06/electric-power-grid-malware.html

38. Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways. (Oakland, CA: Battelle Memorial Institute, 2018).

39. USMC. Destruction by Demolition, Incendiaries and Sabotage. Field Training Manual, Fleet Marine Force. (Boulder, CO: Paladin Press, 1942).

40. Inspire Magazine, Issue 17, Summer, 2017, p. 6.

41. Department of Justice (DOJ). Report on the Availability of Bomb Making Information. (Washington, DC: US Department of Justice, 1997).

42. Major H. von Dach Bern. Total Resistance: A Swiss Army Guide to Guerrilla Warfare and Underground Operations. (Boulder, CO: Paladin Press. 1965).

43. Majorie Van Leijen. "Freight shifts from rail to road due to Basel-Karlsruhe disruption." Rail.com. August 22, 2017. https://www.railfreight.com/business/2017/08/22/freight-shift-from-rail-to-road-due-to-basel-karlsruhe-disruptions/ (accessed July 3, 2018).

44. University of Denver. "Building and Maintaining Infrastructure." Transportation Institute. 2015. https://www.du.edu/transportation/media/documents/industry-insights/1-du-building-and-maintaining-infrastructure.pdf (accessed July 1, 2019).

45. James Surowiecki. "System Overload". The New Yorker. April 18, 2016. https://www.newyorker.com/magazine/2016/04/18/inside-americas-infrastructure-problem (accessed June 15, 2018).

46. William M. Leavitt and John J. Kiefer. "Infrastructure Interdependency and the Creation of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans." Public Works Management & Policy. Vol. 10, no. 4: pp. 306–314, 2006. https://doi.org/10.1177/1087724X06289055 (accessed March 12, 2018).

47. Felix Rioja. “What is the value of Infrastructure Maintenance?” Infrastructure and Land Policies. (Cambridge, MA: Lincoln Institute of Land Policy, 2013). https://www.lincolninst.edu/sites/default/files/pubfiles/what-is-the-value-of-infrastructure-maintenance_0.pdf (accessed June 15, 2018).

48. Robert Puentes. Why Infrastructure Matters: Rotten Roads, Bum Economy. January 20, 2015. Washington Examiner. https://www.brookings.edu/opinions/why-infrastructure-matters-rotten-roads-bum-economy/ (accessed June 15, 2018).

49. National Transportation Safety Board. (NTSB). Collapse of I-35W Highway Bridge, Minneapolis, Minnesota, August 1, 2007. Highway Accident Report NTSB/HAR-08/03. Washington, DC. 2008.

50. Federal Highway Administration. “Questions and Answers on The National Bridge Inspection Standards 23 CFR 650 Subpart C, 2017. Bridges & Structures.” 2017. Https://www.Fhwa.Dot.Gov/Bridge/Nbis/Index.Cfm (accessed June 15, 2018).

51. Code of Federal Regulations. “Questions and Answers on the National Bridge Inspection Standards 23.” CFR 650 Subpart C, 2017. https://www.govinfo.gov/content/pkg/CFR-2011-title23-vol1/pdf/CFR-2011-title23-vol1-part650-subpartC.pdf (accessed June 15, 2018).

52. Transportation Research Board (TRB). Making Transportation Tunnels Safe and Secure. TCRP Report 86, volume 12. (Washington, D.C.: Transportation Research Board of the National Academies. 2006).

53. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

54. Brian M. Jenkins. The Challenge of Protecting Transit and Passenger Rail: Understanding How Security Works Against Terrorism. (San Jose, CA: Mineta Transportation Institute, 2017)

55. Federal Bureau of Investigation (FBI). Bay Area Terrorism Working Group Briefing. Oakland, California. April 14, 2004.

56. Federal Bureau of Investigation (FBI). Bay Area Terrorism Working Group Briefing. Oakland, California. April 14, 2004.

57. Sarah Leivesley. “Emergency Preparedness UK: Case Study London Bombings, July 2005.” Paper delivered at the NATO Joint STS-CNAD Workshop, Ericeira, Portugal, March 2–4, 2006.

58. Department of Homeland Security. Bomb-making Materials Awareness Program. 2018. https://www.dhs.gov/bmap (accessed June 15, 2018).

59. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security.

(Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

60. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

61. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

62. Brian M. Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed January 15, 2019).

63. Demian Bulwa. “BART admits 77% of train cameras are fake or don’t work.” SF Gate. February 9, 2016. https://www.sfgate.com/crime/article/BART-admits-77-percent-of-train-cameras-are-fake-6818459.php (accessed June 15, 2018).

64. Evan Sernoffsky and Michael Cabanatuan. ”BART takes heat but defends fake cameras.” SF Gate. January 14, 2016. https://www.sfgate.com/crime/article/Use-of-decoy-cameras-seems-to-set-BART-apart-6760101.php (accessed June 15, 2018).

65. Gemma Mullin. “Terror Atrocity: What Happened in The 7/7 London Bombings, How Many Victims Were There in The Terror Attack and Who Were the Bombers?” The Sun. July 7, 2017. https://www.thesun.co.uk/news/3966186/july-7-london-bombings-victims-terror-attack-bombers/ (accessed July 1, 2018).

66. Laura Anthony. “BART security cameras now keeping eye on all train cars.” ABC 7-KGO. June 28, 2017. http://abc7news.com/traffic/bart-security-cameras-now-keeping-eye-on-all-trains/2161217/ (accessed June 15, 2018).

67. Evan Sernoffsky and Michael Cabanatuan. ”BART takes heat but defends fake cameras.” SF Gate. January 14, 2016. https://www.sfgate.com/crime/article/Use-of-decoy-cameras-seems-to-set-BART-apart-6760101.php (accessed June 15, 2018).

68. Kashmir Hill. “London’s amazingly explicit surveillance state mascot for the 2012 Olympics has a huge camera eye that ‘records everything.’” Forbes. May 17, 2012. https://www.forbes.com/sites/kashmirhill/2012/05/17/londons-amazingly-explicit-surveillance-state-mascot-for-the-2012-olympics-has-a-huge-camera-eye-that-records-everything/#553dae3d2ea0 (accessed June 15, 2018).

69. Viseum. “Intelligent CCTV Surveillance Systems.” 2018. https://www.viseum.co.uk/cctv-case-studies/olympics-cctv/ (accessed June 15, 2018).

70. Viseum. “Intelligent CCTV Surveillance Systems.” 2018. https://www.viseum.co.uk/cctv-case-studies/olympics-cctv/ (accessed June 15, 2018).

71. Matthew Taylor. “London 2012 crowds to bring Olympic challenge for CCTV team.” The Guardian. May 13, 2012. https://www.theguardian.com/world/2012/may/13/

london-2012-olympic-cctv (accessed June 15, 2018).

72. Stephen Graham. “Olympics 2012 security: welcome to lockdown London.” The Guardian. March 12, 2012. https://www.theguardian.com/sport/2012/mar/12/london-olympics-security-lockdown-london (accessed June 15, 2018).

73. Department of Homeland Security (DHS). Baseline Capabilities for State and Major Urban Area Fusion Centers. October, 2008. Washington, DC: DHS.

74. Barack Obama. Presidential Policy Directive-8, March 30, 2008. (Washington, DC: The White House).

75. Nicholas Hambridge, Arnold M. Howitt and David W. Giles. “Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies.” Homeland Security Affairs 13, Article 2, April 2017. https://www.hsaj.org/articles/13773 (accessed October 12, 2018).

76. Department of Homeland Security. (DHS). “Critical Infrastructure Sectors.” Retrieved from https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed October 12, 2018).

77. Barack Obama. Presidential Policy Directive-21, February 12, 2013. (Washington, DC: The White House).

78. H.J. Poole. The Last Hundred Yards: The NCO’s Contribution to Warfare. p. xvi. (Emerald Isle, NC: Posterity Press, 1997).

79. Major John L. Plaster, Sniping in the Trenches: World War I and the Birth of Modern Sniping. (Boulder, CO.: Palladin Press, 2017).

80. H. J. Poole. The Last Hundred Yards: The NCO’s Contribution to Warfare. p. xvi. (Emerald Isle, NC: Posterity Press, 1997).

81. Frank W. Abagnale. The Art of the Steal. (New York, NY: Broadway Books, 2001).

82. Askmen. “The Spanish Prisoner: Top Ten Classic Cons.” No date. https://www.askmen.com/top_10/entertainment/top-10-classic-cons_2.html (accessed July 1, 2019).

83. Stephanie Yang. “5 Years Ago Bernie Madoff Was Sentenced to 150 Years In Prison – Here’s How His Scheme Worked.” Business Insider. July 1, 2014. https://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7 (accessed July 1, 2019).

84. Special Operations Executive (SOE). Secret Operations Manual. (Boulder, CO: Paladin Press, 1993).

85. Mary Comerico. Disaster Hits Home: New Policy for Urban Housing Recovery.

(Berkeley, CA: University of California Press, 1998).

86. Mary Comerio. “Disaster Recovery and Community Renewal: Housing Approaches,” Cityscape: A Journal of Policy Development and Research. 16, no. 2 (2014): 51–68.

87. Amy Smithson and Leslie-Ann Levy. Ataxia: The Chemical and Biological Terrorism Threat and the US Response. Stimson Report 35. (Washington, DC: Stimson Center, October 9, 2000). https://www.stimson.org/content/ataxia-chemical-and-biological-terrorism-threat-and-us-response (accessed August 1, 2001).

88. Titan Systems. Arlington County: After Action Report on the Response to the September 11 Terrorist Attack on the Pentagon. 2002. (Washington, DC: Department of Justice, Office of Justice Programs, Office for Domestic Preparedness, under Contract Number GS10F0084K, Order Number 2001F_341.) http://www.au.af.mil/au/awc/awcgate/9-11/pentagonafteractionreport.pdf (accessed June 3, 2019).

89. George W. Bush. Homeland Security Presidential Directive-5. February 28, 2003. (Washington, D.C.: The White House.)

90. Brian M. Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed January 15, 2019).

91. Peter Bergen. “Truck attacks – a frightening tool of terror, with a history.” CNN. January 9, 2017. https://www.cnn.com/2016/07/14/opinions/truck-attacks-tactic-analysis-bergen/ (accessed January 15, 2019).

92. Brian M. Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed January 15, 2019).

93. BBC News. “Nice attack: what we know about the Bastille Day killings.” August 19, 2016. https://www.bbc.com/news/world-europe-36801671 (accessed January 15, 2019).

94. BBC News. “Nice attack: what we know about the Bastille Day killings.” August 19, 2016. https://www.bbc.com/news/world-europe-36801671 (accessed January 15, 2019).

95. Hossam Wahbeh. “Truck attack in Nice.” Al Jazeera. July 10, 2018. https://www.aljazeera.com/programmes/aljazeeraworld/2018/07/truck-attack-nice-180710132318265.html (accessed January 15, 2019).

96. BBC News. “Nice attack: what we know about the Bastille Day killings.” August 19, 2016. https://www.bbc.com/news/world-europe-36801671 (accessed January 15, 2019).

97. TSA, Office of Security Policy and Industry. (U) Vehicle Ramming Attacks: Threat Landscape, Indicators, and Countermeasures. Washington, DC: TSA, 2017. https://info.publicintelligence.net/TSA-VehicleRamming.pdf (accessed January 15, 2019).

98. BBC News. “Nice attack: what we know about the Bastille Day killings.” August 19, 2016. https://www.bbc.com/news/world-europe-36801671 (accessed January 15, 2019).

99. Sarah Leivesley. “Emergency Preparedness UK: Case Study London Bombings, July 2005.” Paper delivered at the NATO Joint STS-CNAD Workshop, Ericeira, Portugal, March 2–4, 2006.

100. Brian M. Jenkins and Jean-François Clair. Trains, Concert Halls, Airports, and Restaurants—All Soft Targets: What the Terrorist Campaign in France and Belgium Tells Us about the Future of Jihadist Terrorism in Europe. (San Jose, CA: Mineta Transportation Institute, 2016). http://transweb.sjsu.edu/research/trains-concert-halls-airports-and-restaurants—all-soft-targets-what-terrorist-campaign (accessed June 15, 2018).

101. Jackson, Brian A., and others. Aptitude for Destruction, vol. 1 & 2. (Santa Monica, CA: RAND Corporation, 2005).

102. Foreman, Dave. Eco Defense: A Field Guide to Moneywrenching. (Chico, CA: Abbzug Press, 1993).

103. Brian Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018), http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed May 3, 2019).

104. Frances Edwards Winslow and John Walmsley. “Metropolitan Medical Strike Team Systems: Responding to the Medical Demands of WMD/NBC Events”. In Ali Farazmand (ed.), Handbook of Crisis and Emergency Management. (New York: Marcel Dekker, Inc., 2001).

105. United Nations. “Weapons of mass disruption.” UNTerm. UN Headquarters. No date. https://unterm.un.org/unterm/Display/record/UNHQ/weapon_of_mass_disruption/AFBBCFB9D20742FB85256BD4005C6AED (accessed August 30, 2019).

106. Special Operations Executive (SOE). How to be a Spy. Toronto, Canada: Dundurn Press, 2001/2004.

107. Mark R. Carter, and others. Effects of Catastrophic Events on Transportation System Management And Operations- Howard Street Tunnel Fire, Baltimore City, Maryland, July 18, 2001: Final Report: Findings. U.S. Department of Transportation ITS Joint Program Office, July 18, 2001. https://www.hsdl.org/?view&did=455130 (accessed February 15, 2008).

108. US Fire Administration (USFA). “CSX Tunnel Fire.” July, 2001. http://www.usfa.fema.gov/downloads/pdf/publications/tr-140.pdf (accessed February 17, 2014).

109. US Fire Administration. CSX Tunnel Fire, Baltimore, Maryland. USFR-TA-140. July, 2001. https://www.usfa.fema.gov/downloads/pdf/publications/tr-140.pdf (accessed February 17, 2014).

110. Stephen Ginsberg. “NTSB Faults Baltimore, CSX in 2001 Tunnel Fire, Report Calls Coordination Inadequate.” Washington Post. January 6, 2005. http://www.washingtonpost.com/wp-dyn/articles/A51908-2005Jan5.html?noredirect=on (accessed February, 2012).

111. Frances L. Edwards and Daniel C. Goodrich. Introduction to Transportation Security. (Boca Raton FL: CRC Press/ Taylor and Francis, 2013).

112. San Jose Office of Emergency Services. “After Action Report: Transit Mall Collapse.” City of San Jose, CA, November 3, 1992.

113. Karen de Sa. “A&T raises reward in phone-outage sabotage to $250,000.” Mercury News. April 10, 2009, https://www.mercurynews.com/2009/04/10/att-raises-reward-in-phone-outage-sabotage-to-250000/ (accessed June 15, 2019).

114. California Emergency Services Association. (CESA) “AT&T Denial of Service Attack.” Presentation at the Google Campus, Mountain View, CA. June 10, 2009.

115. Silicon Valley Emergency Communication Service (SVECS). “When All Else Fails: AT&T Failure.” SVECS meeting, City of Santa Clara Senior Center. January 23, 2010.

116. Silicon Valley Emergency Communication Service (SVECS). “When All Else Fails: AT&T Failure.” SVECS meeting, City of Santa Clara Senior Center. January 23, 2010.

117. Benjamin Mueller, William Rashbaum, and Al Baker. “Terror attack kills 8 and injures 11 in Manhattan.” The New York Times, October31, 2017. https://www.nytimes.com/2017/10/31/nyregion/police-shooting-lower-manhattan.html (accessed June 25, 2019).

118. Benjamin Mueller, William Rashbaum, and Al Baker. “Terror attack kills 8 and injures 11 in Manhattan.” The New York Times, October31, 2017. https://www.nytimes.com/2017/10/31/nyregion/police-shooting-lower-manhattan.html (accessed June 25, 2019).

119. Evan Simko-Bednarski. “NYC terror suspect Sayfullo Saipov was surveilled by the government for three years before his alleged attack. Now he wants access to the material.” CNN, March 18, 2019. https://www.cnn.com/2019/03/18/us/nyc-terror-suspect-surveillance-sayfullo-saipov/index.html (accessed May 29, 2019).

120. Benjamin Weiser. “Man Charged in Manhattan Truck Attack That Killed 8 People

Speaks Out at Hearing." New York Times, June 22, 2018. https://www.nytimes.com/2018/06/22/nyregion/manhattan-truck-attack-trial.html (accessed July 1, 2019).

121. Department of Homeland Security. (DHS). Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places. p. 1. No date. Retrieved from https://www.dhs.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF

122. Brian Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed May 3, 2019).

123. Brian Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. p. 16. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed May 3, 2019).

124. Laura Anthony. "BART security cameras now keeping eye on all train cars." ABC 7-KGO. June 28, 2017. http://abc7news.com/traffic/bart-security-cameras-now-keeping-eye-on-all-trains/2161217/ (accessed June 15, 2018).

125. Street Smart Campaign. Street Smart Pedestrian and Bicycle Safety Public Awareness Campaign, Fall 2007 And Spring 2008: Annual Report and Campaign Summary. 2008. http://www.bestreetsmart.net/docs/2008/2008-annual-report.pdf (accessed June 15, 2018).

126. Department of Homeland Security. (DHS). Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places. No date. https://www.dhs.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF (accessed May 11, 2019).

127. Kathy H. Lococo, and others. Pedal Application Errors. (Report No. DOT HS 811 597). (Washington, DC: National Highway Traffic Safety Administration, March 2012).

128. Judith Mwakalonge, Saidi Siuh, and Jamario White. "Distracted walking: Examining the extent to pedestrian safety problems." Journal of Traffic and Transportation Engineering (English Edition), Volume 2, Issue 5, October 2015, Pages 327–337. https://doi.org/10.1016/j.jtte.2015.08.004 (accessed July 1, 2019).

129. Brian Jenkins and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed May 3, 2019).

130. Department of Homeland Security. (DHS). Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places. No date. https://www.dhs.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF (accessed May 11, 2019).

BIBLIOGRAPHY

Abagnale, Frank W. The Art of the Steal. New York, NY: Broadway Books, 2001.

American Civil Liberties Union (ACLU). “Surveillance cameras and the attempted London attack”. 2018. https://www.aclu.org/other/surveillance-cameras-and-attempted-london-attacks (accessed June 5, 2018).

American Society of Civil Engineers. 2017 Infrastructure Report Card. 2017. https://www.infrastructurereportcard.org/ (accessed June 25, 2018).

Anthony, Laura. “BART security cameras now keeping eye on all train cars.” ABC 7-KGO. June 28, 2017. http://abc7news.com/traffic/bart-security-cameras-now-keeping-eye-on-all-trains/2161217/ (accessed June 15, 2018).

Askmen. “The Spanish Prisoner: Top Ten Classic Cons.” No date. https://www.askmen.com/top_10/entertainment/top-10-classic-cons_2.html (accessed July 1, 2019).

Associated Press. “Eight remain hospitalized after San Francisco Tour Bus Crash.” The Guardian. November 14, 2015. https://www.theguardian.com/us-news/2015/nov/14/san-francisco-double-decker-tour-bus-crash (accessed June 30, 2018).

BBC News. “Nice attack: what we know about the Bastille Day killings.” August 19, 2016. https://www.bbc.com/news/world-europe-36801671 (accessed January 15, 2019).

BBC News. “London attack: police know Identities of killers.” June 5, 2017. https://www.bbc.co.uk/news/uk-40155451 (accessed June 5, 1018).

Battelle Memorial Institute. All Aboard for Safety: Building Smarter Safer Railways. (Oakland, CA: Battelle Memorial Institute, 2018).

Bean, Hamilton, Lisa Keränen, and Margaret Durfy. “This is London: Cosmopolitan Nationalism and the Discourse of Resilience in the Case of the 7/7 Terrorist Attacks.” Rhetoric and Public Affairs, vol. 14, no. 3, pp. 427–464. 2011.

Bergen, Peter. “Truck attacks – a frightening tool of terror, with a history.” CNN. January 9, 2017. https://www.cnn.com/2016/07/14/opinions/truck-attacks-tactic-analysis-bergen/ (accessed January 15, 2019).

Berger, J.M. “How Terrorists Recruit Online and How to Stop It”. Washington, DC: Brookings Institution, November 9, 2015. https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/ (accessed June 12, 2018).

Blinder, Alan, Christina Caron, and John Jeter. “Fatal Amtrak Crash in South Carolina Is New Challenge for Rail Service”. The New York Times. February 4, 2018. https://www.nytimes.com/2018/02/04/us/amtrak-crash-south-carolina.html (accessed July

2, 2018).

Bulwa, Demian. “BART admits 77% of train cameras are fake or don’t work.” SF Gate. February 9, 2016. https://www.sfgate.com/crime/article/BART-admits-77-percent-of-train-cameras-are-fake-6818459.php (accessed June 15, 2018).

Burgen, Steven and Ian Cobain, I. (2017). Barcelona attack: four suspects face court after van driver is shot dead. The Guardian. August 22. https://www.theguardian.com/world/2017/aug/21/police-searching-barcelona-van-driver-shoot-man (accessed June 15, 2018).

Bush, George W. Homeland Security Presidential Directive-5. February 28, 2003. Washington, D.C.: The White House.

CBS News. “4 remain critical after tour bus crash in San Francisco”. November 15, 2015. https://www.cbsnews.com/news/4-remain-in-critical-condition-after-tour-bus-crash-in-san-francisco/ (accessed June 14, 2018).

Cabanatuan, Michael and Kale Williams. “Driver blamed for tour bus crash in SF’s Union Square”. SF Gate. March 23, 2016. https://www.sfgate.com/bayarea/article/Driver-blamed-for-tour-bus-crash-in-SF-s-Union-6994435.php (accessed June 30, 2018).

Carter, Mark R., Mark P. Howard, Nicholas Owens, David Register, Jason Kennedy, Kelley Pecheux, and Aaron Newton. “Effects of Catastrophic Events On Transportation System Management and Operations- Howard Street Tunnel Fire Baltimore City, Maryland, July 18, 2001: Final Report: Findings.” U.S. Department of Transportation ITS Joint Program Office, July 18, 2001. https://www.hsdl.org/?view&did=455130 (accessed February 15, 2008).

California Emergency Services Association. (CESA). “AT&T Denial of Service Attack.” Presentation at the Google Campus, Mountain View, CA. June 10, 2009.

Code of Federal Regulations. “Questions and Answers on the National Bridge Inspection Standards 23.” CFR 650 Subpart C, 2017. https://www.govinfo.gov/content/pkg/CFR-2011-title23-vol1/pdf/CFR-2011-title23-vol1-part650-subpartC.pdf (accessed June 15, 2018).

Comerico, Mary. Disaster Hits Home: New Policy for Urban Housing Recovery. Berkeley, CA: University of California Press, 1998.

Comerio, Mary. “Disaster Recovery and Community Renewal: Housing Approaches,” Cityscape: A Journal of Policy Development and Research. 16, no. 2 (2014): pp. 51–68.

Davis, Mike. Buda’s Wagon: A Brief History of the Car Bomb. New York: Verso, 2007.

de Sa, Karen. AT&T raises reward in phone-outage sabotage to $250,000. April 10,

2009. Mercury News. https://www.mercurynews.com/2009/04/10/att-raises-reward-in-phone-outage-sabotage-to-250000/ (accessed June 15, 2018).

Department of the Army. Boobytrapping, Field Manual 531. Washington, DC: Department of the Army, 1965.

Department of the Army. Improvised Munitions Handbook. Technical Manual 31-210. Washington, DC: Department of the Army, 1969.

Department of the Army. Unconventional Warfare Devices and Techniques: Technical Manual 31-200-1. Washington, DC: Department of the Army, 1963.

Department of Homeland Security (DHS). Baseline Capabilities for State and Major Urban Area Fusion Centers. October, 2008. Washington, DC: DHS.

Department of Homeland Security (DHS). Bomb-making Materials Awareness Program. 2018. https://www.dhs.gov/bmap (accessed June 15, 2018).

Department of Homeland Security. (DHS). “Critical Infrastructure Sectors.” No date. https://www.dhs.gov/cisa/critical-infrastructure-sectors (accessed October 12, 2018).

Department of Homeland Security. (DHS). Vehicle Ramming: Security Awareness for Soft Targets and Crowded Places. No date. Retrieved from https://www.dhs.gov/sites/default/files/publications/Vehicle%20Ramming%20-%20Security%20Awareness%20for%20ST-CP.PDF (accessed January 15, 2019).

Department of Justice (DOJ). Report on the Availability of Bomb Making Information. (Washington, DC: US Department of Justice, 1997).

Dupont. Blaster’s Manual, 15th edition. Wilmington, DE: Dupont Sales Development Division, 1969.

Dupont, E.I. de Nemours. Blaster’s Manual. Wilmington, De: Dupont & Company, Incorporated, 1922. https://the-eye.eu/public/Books/campdivision.com/Sensitive/Anarchy%20Folder/Explosives%20%26%20Incendiaries/Demolition%2C%20Blasting%2C%20Sabotage/Dupont%20Blasters%20Handbook%201922%20ed.pdf (accessed July 1, 2019).

Edwards, Frances L. and Daniel C. Goodrich. Introduction to Transportation Security. Boca Raton FL: CRC Press/ Taylor and Francis, 2013.

Federal Bureau of Investigation (FBI). Bay Area Terrorism Working Group Briefing. Oakland, California. April 14, 2004.

Federal Highway Administration. 2017. “Questions and Answers on The National Bridge Inspection Standards 23 CFR 650 Subpart C, 2017. Bridges & Structures.” Https://

www.Fhwa.Dot.Gov/Bridge/Nbis/Index.Cfm (accessed June 15, 2018).

Foreman, Dave. Eco Defense: A Field Guide to Monkeywrenching. Chico, CA: Abbzug Press, 1993.

Ginsberg, Stephen. “NTSB Faults Baltimore, CSX in 2001 Tunnel Fire, Report Calls Coordination Inadequate.” Washington Post. January 6, 2005. http://www.washingtonpost.com/wp-dyn/articles/A51908-2005Jan5.html?noredirect=on (accessed February, 2012).

Graham, Stephen. “Olympics 2012 security: welcome to lockdown London.” The Guardian. March 12, 2012. https://www.theguardian.com/sport/2012/mar/12/london-olympics-security-lockdown-london (accessed June 15, 2018).

Hambridge, Nicholas, Arnold M. Howitt and David W. Giles. “Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies.” Homeland Security Affairs 13, Article 2, April 2017. https://www.hsaj.org/articles/13773 (accessed October 12, 2018).

Hill, Kashmir. “London’s amazingly explicit surveillance state mascot for the 2012 Olympics has a huge camera eye that ‘records everything.’” Forbes. May 17, 2012. https://www.forbes.com/sites/kashmirhill/2012/05/17/londons-amazingly-explicit-surveillance-state-mascot-for-the-2012-olympics-has-a-huge-camera-eye-that-records-everything/#553dae3d2ea0 (accessed June 15, 2018).

Horwitz, Jeff. “Who’s at fault in Amtrak Crash?” Associated Press/ Miami Herald, February 10, 2018. https://www.chicagotribune.com/nation-world/ct-amtrak-crash-payment-agreements-20180210-story.html (accessed June 13, 2018).

Inspire Magazine, Issue 17, Summer, 2017, p. 6.

IFSEC Global. “Role of CCTV Cameras: Public, Privacy and Protection”. January 1, 2014. https://www.ifsecglobal.com/role-cctv-cameras-public-privacy-protection/ (accessed June 14, 2018).

Jackson, Brian A. , John C. Baker, Peter Chalk, Kim Cragin, John V. Parachini, and Horacio R. Trujillo. Aptitude for Destruction, vol. 1 & 2. Santa Monica, CA: RAND Corporation, 2005.

Jenkins, B.M. Protecting Surface Transportation Systems and Patrons from Terrorist Activities. San Jose, CA.: Mineta Transportation Institute. 1997. http://transweb.sjsu.edu/research/protecting-surface-transportation-systems-and-patrons-terrorist-activities-0 (accessed June 15, 2018).

Jenkins, Brian M. Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. Report 01-07. San Jose, CA: Mineta Transportation Institute. 2001

http://transweb.sjsu.edu/MTIportal/research/publications/summary/0107.html (accessed July 15, 2018).

Jenkins, Brian M. The Challenge of Protecting Transit and Passenger Rail: Understanding How Security Works Against Terrorism. (San Jose, CA: Mineta Transportation Institute, 2017) http://transweb.sjsu.edu/research/challenge-protecting-transit-and-passenger-rail-understanding-how-security-works-against (accessed July 15, 2018).

Jenkins, Brian M. and Bruce Butterworth. An Analysis of Vehicle Ramming as a Terrorist Tactic. (San Jose, CA: Mineta Transportation Institute, 2018). http://transweb.sjsu.edu/research/Analysis-Vehicle-Ramming-Terrorist-Threat (accessed January 15, 2019).

Jenkins, Brian M. and Bruce Butterworth. Terrorist Vehicle Attacks on Public Surface Transportation Targets. San Jose, CA: Mineta Transportation Institute, 2017. http://transweb.sjsu.edu/research/Terrorist-Vehicle-Attacks-Public-Surface-Transportation-Targets (accessed June 15, 2018).

Jenkins, Brian M. & Bruce Butterworth. The Threat to Air and Ground Transportation Posed by Mentally Disordered Assailants. San Jose, CA: Mineta Transportation Institute, 2017. http://transweb.sjsu.edu/research/Threat-Air-and-Ground-Transportation-Posed-Mentally-Disordered-Assailants (accessed June 15, 2018).

Jenkins, Brian M. and Jean-François Clair. Trains, Concert Halls, Airports, and Restaurants—All Soft Targets: What the Terrorist Campaign in France and Belgium Tells Us about the Future of Jihadist Terrorism in Europe. San Jose, CA: MTI, 2016. http://transweb.sjsu.edu/research/trains-concert-halls-airports-and-restaurants—all-soft-targets-what-terrorist-campaign (accessed June 15, 2018).

Jenkins, Brian M. and Frances L. Edwards-Winslow. Saving City Lifelines. Mineta Transportation Institute, 2002. http://transweb.sjsu.edu/research/saving-city-lifelines-lessons-learned-9-11-terrorist-attacks (accessed July 15, 2018).

Khandelwal, Swati. “Dangerous malware discovered that can take down electric power grids.” Hacker News. June 12, 2017. https://thehackernews.com/2017/06/electric-power-grid-malware.html

Lawless, Jill. “Surveillance in the U.K. ‘just kept expanding’ after the London bombings.” Business Insider. 2015. http://www.businessinsider.com/surveillance-in-the-uk-just-kept-expanding-after-the-london-bombings-2015-7 (accessed July 1, 2018).

Leivesley, Sarah. “Emergency Preparedness UK: Case Study London Bombings, July 2005.” Paper delivered at the NATO Joint STS-CNAD Workshop, Ericeira, Portugal, March 2–4, 2006.

Leavitt, William M. and John J. Kiefer. “Infrastructure Interdependency and the Creation

of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans." Public Works Management & Policy. Vol. 10, no. 4: pp. 306–314, 2006. https://doi.org/10.1177/1087724X06289055 (accessed March 12, 2018).

Lococo, Kathy H., Loren Staplin, Carol A. Martell, and Kathy J. Sifrit. Pedal Application Errors. (Report No. DOT HS 811 597). (Washington, DC: National Highway Traffic Safety Administration, March 2012).

Lulushi, Albert. Donovan's Devils: OSS Commandos Behind Enemy Lines- Europe, World War II. New York: Arcade Publishing, 2018.

Mueller, Benjamin, William Rashbaum, Al Baker. "Terror attack kills 8 and injures 11 in Manhattan." The New York Times. October31, 2017. https://www.nytimes.com/2017/10/31/nyregion/police-shooting-lower-manhattan.html (accessed June 25, 2019).

Mullin, Gemma. "Terror Atrocity: What Happened in The 7/7 London Bombings, How Many Victims Were There in The Terror Attack and Who Were the Bombers?" The Sun. July 7, 2017. https://www.thesun.co.uk/news/3966186/july-7-london-bombings-victims-terror-attack-bombers/ (accessed July 1, 2018).

Mwakalonge, Judith, Saidi Siuh, and Jamario White. "Distracted Walking: Examining the Extent to Pedestrian Safety Problems." Journal of Traffic and Transportation Engineering (English Edition), Volume 2, Issue 5, October 2015, pp. 327–337. https://doi.org/10.1016/j.jtte.2015.08.004 (accessed July 1, 2019).

National Transportation Safety Board. (NTSB). Collapse of I-35W Highway Bridge, Minneapolis, Minnesota, August 1, 2007. Highway Accident Report NTSB/HAR-08/03. Washington, DC, 2008.

Obama, Barak. Presidential Policy Directive-8, March 30, 2008. Washington, DC: The White House.

Obama, Barak. Presidential Policy Directive-21, February 12, 2013. Washington, DC: The White House.

Palmer, Annie. "AI surveillance cameras would soon identify faces in a crowd with 99 percent accuracy." Daily Mail. February 16, 2018. http://www.dailymail.co.uk/sciencetech/article-5401325/CCTV-cameras-soon-face-recognition-technology.html (accessed June 14, 2018).

Park, Madison & Holly Yan. "What is Positive Train Control, and could it have prevented the Amtrak crash?" CNN. February 5, 2018. https://www.cnn.com/2018/02/05/us/positive-train-control-explainer/index.html (accessed July 12, 2018).

Plaster, Major John L. Sniping in the Trenches: World War I and the Birth of Modern Sniping. Boulder, CO.: Palladin Press, 2017.

Poole, H.J. The Last Hundred Yards: The NCO's Contribution to Warfare. Emerald Isle, NC: Posterity Press, 1997.

Puentes, Robert. Why Infrastructure Matters: Rotten Roads, Bum Economy. January 20, 2015. Washington Examiner. https://www.brookings.edu/opinions/why-infrastructure-matters-rotten-roads-bum-economy/ (accessed June 15, 2018).

Reinares, Fernando. Al-Quaeda's Revenge: The 2004 Madrid Train Bombings. New York: Woodrow Wilson Center Press, Columbia University Press. 2017.

Rioja, Felix. "What is the value of Infrastructure Maintenance?" Infrastructure and Land Policies. (Cambridge, MA: Lincoln Institute of Land Policy, 2013). https://www.lincolninst.edu/sites/default/files/pubfiles/what-is-the-value-of-infrastructure-maintenance_0.pdf (accessed June 15, 2018).

San Jose Office of Emergency Services. "After Action Report: Transit Mall Collapse." City of San Jose, CA, November 3, 1992.

Seattle Times Staff. "4 dead, 2 critically injured in collision between Ride the Ducks vehicle, charter bus on Aurora Bridge." Seattle Times, September 24, 2015. https://www.seattletimes.com/seattle-news/ride-the-ducks-vehicle-collides-with-bus-on-aurora-bridge/ (accessed June 12, 2018).

Sernoffsky, Evan & Michael Cabanatuan. "BART takes heat but defends fake cameras." SF Gate. January 14, 2016. https://www.sfgate.com/crime/article/Use-of-decoy-cameras-seems-to-set-BART-apart-6760101.php (accessed June 15, 2018).

Simko-Bednarski, Evan. "NYC terror suspect Sayfullo Saipov was surveilled by the government for three years before his alleged attack. Now he wants access to the material." CNN, March 18, 2019. https://www.cnn.com/2019/03/18/us/nyc-terror-suspect-surveillance-sayfullo-saipov/index.html (accessed May 29, 2019).

Smithson, Amy and Leslie-Ann Levy. Ataxia: The Chemical and Biological Terrorism Threat and the US Response. Stimson Report 35. Washington, DC: Stimson Center, October 9, 2000. https://www.stimson.org/content/ataxia-chemical-and-biological-terrorism-threat-and-us-response (accessed August 1, 2001).

Special Operations Executive (SOE). How to be a Spy. Toronto, Canada: Dundurn Press, 2001/2004.

Special Operations Executive (SOE). Secret Operations Manual. Boulder, CO: Palladin Press, 1993.

Street Smart Campaign. Street Smart Pedestrian and Bicycle Safety Public Awareness Campaign, Fall 2007 And Spring 2008: Annual Report and Campaign Summary. 2008. http://www.bestreetsmart.net/docs/2008/2008-annual-report.pdf (accessed June 15, 2018).

Surowiecki, James. “System Overload”. The New Yorker. April 18, 2016. https://www.newyorker.com/magazine/2016/04/18/inside-americas-infrastructure-problem (accessed June 15, 2018).

Silicon Valley Emergency Communication Service (SVECS). “When All Else Fails: AT&T Failure.” SVECS meeting, City of Santa Clara Senior Center. January 23, 2010.

Tait, Melissa. Toronto van attack: How you can help and what we know so far. The Globe and Mail. April 23, 2018. https://www.theglobeandmail.com/canada/toronto/article-toronto-van-attack-what-we-know-so-far/ (accessed June 15, 2018).

Taylor, Matthew. “London 2012 crowds to bring Olympic challenge for CCTV team.” The Guardian. May 13, 2012. https://www.theguardian.com/world/2012/may/13/london-2012-olympic-cctv (accessed June 15, 2018).

Titan Systems. Arlington County: After Action Report on the Response to the September 11 Terrorist Attack on the Pentagon. 2002. Washington, DC: Department of Justice, Office of Justice Programs, Office for Domestic Preparedness, under Contract Number GS10F0084K, Order Number 2001F_341. http://www.au.af.mil/au/awc/awcgate/9-11/pentagonafteractionreport.pdf (accessed June 3, 2019).

Transportation Research Board (TRB). Making Transportation Tunnels Safe and Secure. TCRP Report 86, volume 12. Washington, D.C.: Transportation Research Board of the National Academies. 2006.

TSA, Office of Security Policy and Industry. (U) Vehicle Ramming Attacks: Threat Landscape, Indicators, and Countermeasures. Washington, DC: TSA, 2017. https://info.publicintelligence.net/TSA-VehicleRamming.pdf (accessed January 15, 2019).

UN Office on Drugs and Crime. The Use of the Internet for Terrorist Purposes. New York, NY: United Nations, November, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (accessed June 15, 2018).

United Nations. “Weapons of mass disruption.” UNTerm. UN Headquarters. No date. https://unterm.un.org/unterm/Display/record/UNHQ/weapon_of_mass_disruption/AFBBCFB9D20742FB85256BD4005C6AED (accessed August 30, 2019).

US Fire Administration (USFA). “CSX Tunnel Fire.” July, 2001. http://www.usfa.fema.gov/downloads/pdf/publications/tr-140.pdf (accessed February 17, 2014).

USMC. Destruction by Demolition, Incendiaries and Sabotage. Field Training Manual, Fleet Marine Force. Boulder, CO: Paladin Press, 1942.

Union Pacific. “Positive Train Control.” https://www.up.com/media/media_kit/ptc/about-ptc/ (accessed July 2, 2019).

University of Denver. “Building and Maintaining Infrastructure.” Transportation Institute. 2015. https://www.du.edu/transportation/media/documents/industry-insights/1-du-building-and-maintaining-infrastructure.pdf (accessed July 1, 2019).

Van Leijen, Majorie. “Freight shifts from rail to road due to Basel-Karlsruhe disruption.” Rail.com. August 22, 2017. https://www.railfreight.com/business/2017/08/22/freight-shift-from-rail-to-road-due-to-basel-karlsruhe-disruptions/ (accessed July 3, 2018).

Viseum. “Intelligent CCTV Surveillance Systems.” 2018. https://www.viseum.co.uk/cctv-case-studies/olympics-cctv/ (accessed June 15, 2018).

von Dach Bern, Major H. Total Resistance: A Swiss Army Guide to Guerrilla Warfare and Underground Operations. Boulder, CO: Paladin Press. 1965.

Wahbeh, Hossam. “Truck attack in Nice.” Al Jazeera. July 10, 2018. https://www.aljazeera.com/programmes/aljazeeraworld/2018/07/truck-attack-nice-180710132318265.html (accessed January 15, 2019).

Weiser, Benjamin. “Man Charged in Manhattan Truck Attack That Killed 8 People Speaks Out at Hearing.” New York Times, June 22, 2018. https://www.nytimes.com/2018/06/22/nyregion/manhattan-truck-attack-trial.html (accessed July 1, 2019).

Winslow, Frances Edwards and John Walmsley. “Metropolitan Medical Strike Team Systems: Responding to the Medical Demands of WMD/NBC Events.” In Ali Farazmand (ed.), Handbook of Crisis and Emergency Management, New York: Marcel Dekker, Inc., 2001.

Yang, Stephanie. “5 Years Ago Bernie Madoff Was Sentenced to 150 Years in Prison – Here’s How His Scheme Worked.” Business Insider. July 1, 2014. https://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7 (accessed July 1, 2019)

Zetter, Kim. “An unprecedented look at Stuxnet, the world’s first digital weapon.” Wired. November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (accessed June 30, 2018).

ABOUT THE AUTHORS

DANIEL C. GOODRICH, MPA, CEM, MEP, CSS

Dan Goodrich is the Senior Transportation Security Scientist with the Mineta Transportation Institute at San Jose State University, and the instructor for "Security Issues for Transportation Professionals" in the Master of Science in Transportation Management program. He is a Certified Emergency Manager, a Master Exercise Practitioner, a Professional Continuity Practitioner and a Certified Security Specialist. He is co-author with Frannie Edwards of *Introduction to Transportation Security*, nine major publications for MTI, as well as a variety of professional articles and book chapters. He provides emergency management planning and training support to Caltrans and Santa Clara Valley Transportation Authority. He is a FEMA-certified instructor for the ICS course suite. He has worked at county government and in the private sector, and has sixteen years' military service, including US Marine Corps Security Forces.

FRANCES L. EDWARDS, MUP, PHD, CEM

Frannie Edwards is Deputy Director of the National Transportation Security Center of Mineta Transportation Institute, and professor and director of the Master of Public Administration program at San Jose State University. She was the governor's appointee for emergency management on the Seismic Safety Commission. Her recent publications include *Housing Recovery After Disaster,* and *Introduction to Transportation Security* with Dan Goodrich*,* as well as reports for MTI, book chapters and journal articles. She has been a member of academic working groups at Harvard University, Stanford University, NATO and the European Union. For 22 years Dr. Edwards was a public administration and emergency management practitioner, including 14 years as the Director of Emergency Preparedness for San Jose, California. She is a certified emergency manager. She has a Ph.D. and M.U.P. from New York University; a M.A. from Drew University; and a Certificate in Hazardous Materials Management from University of California, Irvine.

PEER REVIEW

San José State University, of the California State University system, and the Mineta Transportation Institute (MTI) Board of Trustees have agreed upon a peer review process required for all research published by MTI. The purpose of the review process is to ensure that the results presented are based upon a professionally acceptable research protocol.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Founder, Honorable Norman Mineta (Ex-Officio)
Secretary (ret.),
US Department of Transportation

Chair,
Abbas Mohaddes (TE 2021)
President & COO
Econolite Group Inc.

Vice Chair,
Will Kempton (TE 2022)
Retired

Executive Director,
Karen Philbrick, PhD (Ex-Officio)
Mineta Transportation Institute
San José State University

Richard Anderson (Ex-Officio)
President & CEO
Amtrak

David Castagnetti (TE 2021)
Co-Founder
Mehlman Castagnetti
Rosen & Thomas

Maria Cino (TE 2021)
Vice President
America & U.S. Government
Relations Hewlett-Packard Enterprise

Grace Crunican* (TE 2022)
Retired

Donna DeMartino (TE 2021)
General Manager & CEO
San Joaquin Regional Transit District

Nuria Fernandez* (TE 2020)
General Manager & CEO
Santa Clara Valley
Transportation Authority (VTA)

John Flaherty (TE 2020)
Senior Fellow
Silicon Valley American
Leadership Form

Rose Guilbault (TE 2020)
Board Member
Peninsula Corridor
Joint Powers Board

Ian Jefferies (Ex-Officio)
President & CEO
Association of American Railroads

Diane Woodend Jones (TE 2022)
Principal & Chair of Board
Lea + Elliott, Inc.

Therese McMillan (TE 2022)
Executive Director
Metropolitan Transportation
Commission (MTC)

Bradley Mims (TE 2020)
President & CEO
Conference of Minority
Transportation Officials (COMTO)

Jeff Morales (TE 2022)
Managing Principal
InfraStrategies, LLC

Dan Moshavi, PhD (Ex-Officio)
Dean, Lucas College and
Graduate School of Business
San José State University

Takayoshi Oshima (TE 2021)
Chairman & CEO
Allied Telesis, Inc.

Toks Omishakin (Ex-Officio)
Director
California Department of
Transportation (Caltrans)

Paul Skoutelas (Ex-Officio)
President & CEO
American Public Transportation
Association (APTA)

Dan Smith (TE 2020)
President
Capstone Financial Group, Inc.

Beverley Swaim-Staley (TE 2022)
President
Union Station Redevelopment
Corporation

Jim Tymon (Ex-Officio)
Executive Director
American Association of
State Highway and Transportation
Officials (AASHTO)

Larry Willis (Ex-Officio)
President
Transportation Trades
Dept., AFL-CIO

(TE) = Term Expiration
* = Past Chair, Board of Trustees

Directors

Karen Philbrick, Ph.D.
Executive Director

Hilary Nixon, Ph.D.
Deputy Executive Director

Asha Weinstein Agrawal, Ph.D.
Education Director
National Transportation Finance
Center Director

Brian Michael Jenkins
National Transportation Security
Center Director

Research Associates Policy Oversight Committee

Jan Botha, Ph.D.
Civil & Environmental Engineering
San José State University

Katherine Kao Cushing, Ph.D.
Enviromental Science
San José State University

Dave Czerwinski, Ph.D.
Marketing and Decision Science
San José State University

Frances Edwards, Ph.D.
Political Science
San José State University

Taeho Park, Ph.D.
Organization and Management
San José State University

Christa Bailey
Martin Luther King, Jr. Library
San José State University

MINETA TRANSPORTATION INSTITUTE