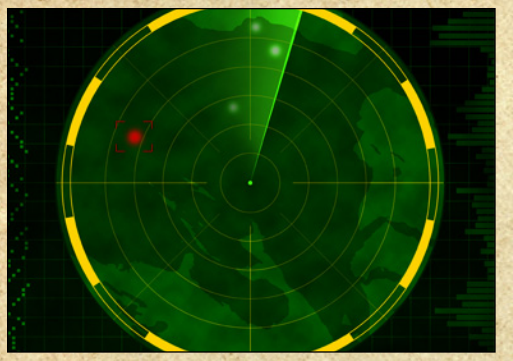
domestic preparedness .com

DomPrep Journal

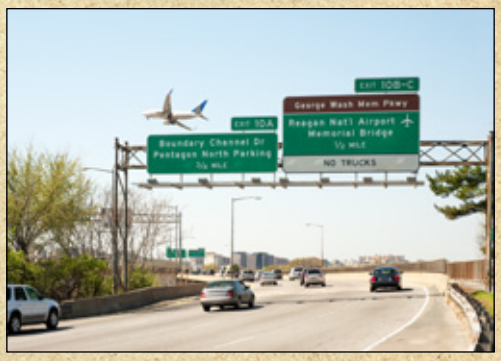
Subscribe Volume 13, Issue 11, November 2017

Unmanned Aircraft Systems – On the Way to the Jetsons' Era
By Charles J. Guddemi

Drones – Both a Force Multiplier & Headache
By Catherine L. Feinman



Protecting the Homeland From Nefarious Drone Use
By Richard Schoeberl & Kendall J. Smith



Critical Infrastructure Partnerships – Prioritizing Assets
By Christopher Ryan

Freight Rail Safety and Emergency Management
By Kay C. Goss

Chemical Attack on Public Transport – A Likely Scenario
By Zamawang Almemar

Staying "PRIMED" for a Radiation Event
By Grant Coffey

Biothreats – Advocating Action Through Transition
By Robert C. Hutchinson


WE STEPPED UP
SO YOU CAN
STEP BACK.
The new FLIR identiFINDER® R440 lets you scan for radiological threats from farther away to keep you and your community safe.
The new R440 is a lightweight, sourceless RIID that can be operated with one hand and is IP67-rated to survive tough missions. Not only does the 2x2 NaI detector deliver sensitive and fast detection, but it also provides accurate identification during secondary screening. The new 360° EasyFinder™ Mode expedites decision-making to keep you safe.
Learn more at flir.com/R440
FLIR identiFINDER R440
Highly Sensitive, Sourceless Handheld RIID
FLIR

Business Office
P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

IMR GROUP

Featured in This Issue

Pictured on the Cover: (top row) Guddemi, Source: ©iStock.com/Pinkypills; Feinman, Source: ©iStock.com/Zerbor; (second row) Schoeberl & Smith, Source: ©iStock.com/axstokes; Ryan, Source: ©iStock.com/Natalia Bratslavsky; (third row) Goss, Source: ©iStock.com/aapsky; Almemar, Source: ©iStock.com/Ed-Ni-Photo; (bottom row) Coffey, Source: ©iStock.com/hanohiki; Hutchinson, Source: ©iStock.com/shironosov

experience federal resources 2017

6 December, 2017

MARRIOTT WARDMAN PARK
Washington, D.C.

- » Manufacturer Exhibits
- » Product Demonstrations
- » Training
- » Guest Speaker
- » Book Signing
- » And More

ExperienceFR is an exhibition of products and solutions for military, first responders, and law enforcement professionals. A truly one-of-a-kind opportunity for attendees to meet our manufacturer partners, learn about the latest and upcoming solutions, and get up-close product demonstrations and training.

SPECIAL GUEST SPEAKER

SERGEANT DAKOTA MEYER

Medal of Honor Recipient and *New York Times* Best-Selling Author

register now at
www.federalresources.com/experiencefr

FEDERAL RESOURCES®

RAE SYSTEMS by Honeywell

Editorial Remarks

By Catherine L. Feinman

The imaginations of television and filmmakers are often used to create futuristic worlds, with technologies that can be used as tools or as threats. Unmanned aircraft systems (UAS) are one such technology that is now off the screen and often seen in the sky. Like "The Jetsons" of the early 1960s, the airways offer many opportunities to transport people and objects from one place to another. With increased travel and transport, though, emergency preparedness, response, and resilience professionals must address the potential benefits of this technology as well as regulations and enforcement issues that could hinder daily and disaster operations. In a worst-case scenario, terrorists could conduct attacks using UAS equipped with explosives, weapons, or dispersal devices for chemical, biological, or radiological materials.

When determining potential threats and vulnerabilities within a particular community, critical infrastructure must be considered. By collaborating within and between jurisdictions, communities can better prioritize assets according to their impact on public safety and quality of life. Freight rail systems that run through multiple jurisdictions are one such critical infrastructure that requires collaborative planning. Similar to television and filmmakers, emergency preparedness and resilience professionals must imagine futuristic scenarios that could affect the health and lives of the communities these rail lines connect. Whether an accidental oil spill or a deliberate chemical attack on public transport, safeguards and plans are needed to address a broad range of potential threat scenarios.

Radiation and biological threats are other scenarios that require careful planning and preparedness efforts to be in place before an incident occurs. Investing in training, education, and equipment for low-probability, high-consequence incidents can improve an understanding of these threats and make uncommon threats less intimidating to address when needed. Once efforts are in place, though, continuity is needed as administrations and personnel change. Otherwise legacy knowledge and investments can be lost. Imagining what could be is an important step in community preparedness, but it cannot and should not supplant what has already been learned from previous incidents and research.

Unmanned Aircraft Systems – On the Way to the Jetsons' Era

By Charles J. Guddemi

Debuting in 1962, "The Jetsons" depicted the family of the future, with people movers, tube travel, vehicles that folded up into brief cases for parking purposes, home computers, internet, microwave ovens, CT x-ray for medical purposes, cellphones, and speed limits of up to 2,500 miles per hour. Fast-forward to today, as roadways become more congested, one logical alternative is to go up. Unmanned aircraft systems bring the nation a step closer to the Jetson way of life.

The National Aeronautics and Space Administration (NASA), coordinating with the Federal Aviation Administration (FAA), currently serves as the lead agency in developing the Unmanned Aircraft Systems (UAS) Traffic Management system to facilitate low-altitude UAS operation. Since they were developed, UAS (commonly known as drones) have transitioned from very large, very expensive products (reserved for military and spy agencies for weapon delivery or reconnaissance purposes) to much smaller, less expensive, commercially available models (used by hobbyists, industry, scientific research, and the first responder community).

Today, UAS are affordable, come in different shapes and sizes, and have different capabilities, which have made them one of the hottest gift ideas for the past couple years. With many benefits and requests for them to be integrated into the national airspace, this trend is expected to continue well into the future. In addition, individuals or groups can use UAS as disruptive technology for nefarious purposes such as invading privacy, advancing criminal enterprises, or conducting terrorist activity.

Potential Threats in the Sky

Still, for many, UAS are seen as toys, something to play with in the backyard or at the local park. For others, this is a new threat to personal security, corporate assets, and critical infrastructure that will force those on the ground to always look up. Two key events sparked debate for further regulation and mitigation of this technology and its capabilities: the UAS incursion onto the south lawn of the White House in January 2015; and the manned, small, low- and slow-flying gyrocopter that landed on the U.S. Capitol's West Lawn in April 2015.

Since the late 1990s and early 2000s, threats from the air and from remote-controlled devices have existed. These threats range from benign to catastrophic. For example, United States Park Police (USPP) officers stationed in New York when the 9/11 attacks occurred encountered a series of incidents that raised great concern.

Within a six-week span in 2001: (1) a paraglider crashed into the Statue of Liberty torch on 23 August; (2) four airplanes crashed into the twin towers in New York City, the Pentagon in Washington, D.C., and a field in Shanksville, Pennsylvania, on 11 September; and (3) a remote-controlled aircraft with a four-foot wingspan washed up on the beach area on the backside of Liberty Island on 1 October. Although the remote aircraft was not found to have been involved in any wrongdoing, the incident sparked new public safety concerns from law enforcement officials in the wake of the 9/11 terrorist attacks.

Technology is approaching that of the Jetsons, and with it the need for regulation, policy, counter capabilities, education, and UAS Traffic Management.

Although UAS was not a significant issue during 9/11, the threat and potential benefits of such technology have evolved since that time. At the Washington, D.C., branch of the USPP, officers respond to many incidents and special events. On 16 September 2013, for example, a multi-aviation response to the Washington Navy Yard shooting required careful coordination to ensure the safety and security of everyone involved. Helicopters certainly played a critical role that day, and remain the best option for some operations (e.g., hoist rescues, medical evacuations, and SWAT insertions). However, under some circumstances, UAS could provide safer, more efficient, and less costly alternatives. In the "fog of war," an overhead perspective offers several benefits:

- Helps clarify communications between many mutual aid assets;
- Identifies the "good guys" and "bad guys";
- Operates when vehicle gridlock on the ground occurs; and
- Conducts building searches through windows and on rooftops.

Enforcement Challenges on the Ground

On 19 June 2014, it became illegal to launch, land, or fly over any National Park Service (NPS) property (under 36 CFR 1.5(f) "Violation of Closure and Public Use Limits: Launching, Landing, or Operation of Unmanned Aircraft"). In collaboration with FAA, U.S. Department of Homeland Security (DHS), United States Capitol Police, and other agencies, USPP recognized the growing threat that UAS could pose and the agency's need to develop plans to mitigate these potential threats. For example, restricted airspace enables USPP to safely operate its aviation assets during large-scale events, but these assets are limited (e.g., helicopter limits ability to get too close to concerts and venues where acoustics can be affected and weather can restrict flight plans).

Despite NPS restrictions, UAS continued to operate on NPS sites in Washington, D.C., New York City, and San Francisco, California. Following is a list of just some of the incidents that occurred in 2015. All of these events highlighted the need for further planning, coordination, and mitigation efforts:

- 26 January – UAS landed on the White House south lawn;
- 15 April – a gyrocopter landed at the U.S. Capitol;

- 12 June – a UAS flew into the chamber of the Jefferson Memorial;
- July – a British national launched a UAS from Liberty Island, circled the Statue of Liberty, took high-resolution video, and landed undetected;
- July – a week after the Liberty Island video, the same British national flew the UAS over the Washington Monument;
- 19 July – a toy quadcopter crashed into the Statue of Liberty; and
- 16 August – a quadcopter flew from Liberty State Park to Liberty Island (after park closure) then to Ellis Island (individual was arrested after NPS personnel saw the aircraft overhead).

Identifying the reasons for these security breaches have helped officials thwart other UAS attempts, but more is still needed. Several reasons that require ongoing planning efforts include the need to:

- Define roles and responsibility for airspace;
- Develop stronger deterrents for violating laws (e.g., in D.C., the fine is only $110);
- Provide screening staff with proper training and education (e.g., screeners at Battery Park are busier than many airport terminals); and
- Ensure that security personnel recognize potential threats (e.g., the UAS taken onto Liberty Island went through an x-ray machine, but was considered a toy).

Multidiscipline Roundtable – Discussing Threats & Benefits

U.S. families may be on the path to becoming the Jetsons of the year 2062, but a lot still has to happen in terms of regulation, policy, counter capabilities, education, and continued development of the UAS Traffic Management. A roundtable discussion with senior subject matter experts representing various communities of interest addressed the benefits and threats the nation faces as this technology evolves and becomes integrated into the daily operations of various industries. Read the proceedings from this event, which features knowledge and advice from the following perspectives: defense; first responder (law enforcement, fire, emergency medical services); intelligence; science, technology, and industry; critical infrastructure; and legal.

Unmanned Aircraft Systems: Benefits & Consequences – Part 1, Proceedings of Roundtable

Charles J. Guddemi served over 25 years for the United States Park Police (USPP). He worked in Washington, D.C., San Francisco, New York, and Philadelphia, rising to the rank of deputy chief. He has worked six presidential inaugurations, serving as the USPP principle planner for the 2013 inauguration. He was responsible for overseeing the safe dedications of the Martin Luther King Jr. and the Americans Veterans Disabled for Life Memorials. Well versed in the Incident Command System, he has served as incident commander, Operations and Planning Section Chief for many of the National Capital Regions largest special events and first amendment demonstrations. After the September 11, 2001, attacks, he designed the in-depth multi-layered security plan for the Statue of Liberty/ Ellis Island Complex, creating mainland screening sites at Battery Park, Manhattan, Liberty State Park in Jersey City, NJ, and a secondary screening facility on Liberty Island prior to entering the Statue of Liberty Monument. The Statue of Liberty/Ellis Island Complex's security plan has served as a model for many of this country's critical infrastructure. He is a graduate of the 237th session of the Federal Bureau of Investigation (FBI) National Academy. He earned a Bachelor's of Art degree in psychology with a minor in business from the State University of New York at Albany.

Drones – Both a Force Multiplier & Headache

By Catherine L. Feinman

Until the federal government decides how to best secure the skies from unmanned aerial systems (UAS), first responders, emergency managers, and public safety professionals will have a big problem to deal with. However, in light of the recent hurricane and wildfires, this technology is also a real game changer for search and rescue and other unforeseen positive uses. Efforts are being made, but more regulation, enforcement, and concepts of operation are still needed to define this transformative technology.

Problems abound with integrating drones into the national airspace system, and countering UAS use by potential attackers – whether criminal, terrorist, or hostile foreign government – is a huge concern. Until authorities figure out how to ensure community safety and commercial benefits, this technology will move beyond the capability of regulators.

The Obama and Trump administrations have both emphasized the need to safely integrate UAS technology into the National Airspace System, while ensuring privacy, civil rights, and civil liberties. On 15 February 2015, The White House released "Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems." That memorandum addressed two key topics: (1) UAS policies and procedures for federal government use – privacy protections, civil rights and liberties protections, accountability, transparency, and report; and (2) multi-stakeholder engagement process. On 2 August 2016, the administration made "New Commitments to Accelerate the Safe Integration of Unmanned Aircraft Systems" and announced $35 million for new UAS research funding through the National Science Foundation over the next five years.

To address issues related to the integration of UAS into the National Airspace System, the White House Office of Science and Technology Policy and the Association for Unmanned Vehicle Systems International brought together key stakeholders of the public and private sectors as well as academia for a workshop on "Drones and the Future of Aviation." Breakout sessions focused on three areas: (1) low-altitude airspace management/UAS traffic management; (2) expanded operations for small UAS; and (3) comprehensive integration to create a smarter National Airspace System.

Trump Administration Plans

The current administration has also expressed plans to expand the integration of UAS as well as enact legislation that counters the illicit use of drones by malicious actors. On 22 June 2017, the White House Office of Science and Technology Policy held another event that brought together industry leaders and federal agencies to address "American Leadership in Emerging Technology." Legislation has been proposed to help close the gap between what the law currently allows and what law enforcement officers need to effectively counter these systems when misused.

In a statement of administration policy on 7 September 2017 – in response to the National Defense Authorization Act for Fiscal Year 2018 – the administration addressed

concern that counter UAS was not included. The statement noted the need to develop a legal framework to guard against misuse and enable effective oversight and privacy protections. The new proposed legislation has a federal focus, but also recognizes that state and local law enforcement agencies may need countermeasures as well. The best and most appropriate way to build capabilities beyond the federal government is still not certain. However, current legislation does not preclude the delegation of their use to appropriate local authorities if used for official use, with federal oversight, and with properly trained operators.

Most recently, on 25 October 2017, The White House released a "Presidential Memorandum for the Secretary of Transportation," which focused on the establishment of a pilot program for UAS integration within 90 days, with proposals being accepted by the FAA by that time. The three-year program has three key objectives: (1) to test and evaluate models for involving state, local, and tribal governments in developing and enforcing federal regulations for UAS; (2) to encourage UAS development and safety testing for new and innovative concepts of operation; and (3) to develop federal guidelines and regulatory decisions for UAS operations. This document expresses the federal government's commitment to promote the following: innovation and economic development; enhancement of transportation and workplace safety; improvement of emergency response as well as search and rescue functions; and the competitive and efficient use of the radio spectrum.

The White House National Security Council also plans to coordinate federal-level working groups on how to look at this emerging technology. The working groups will examine how UAS technologies may be applied effectively from a research and development aspect and from an ethical standpoint. One of the biggest challenges, though, is how to build response policies relevant to federal, state, local, and private actors. To address this challenge, more dialogue is needed with all key government and nongovernment stakeholders.

Input From Various Key Stakeholders

To promote an understanding of threats and capabilities, technology that is being developed, enforcement of rules, threat mitigation activities, and ways to leverage new technology, the Preparedness Leadership Council International hosted a roundtable discussion in June 2017 with senior subject matter experts. These experts represented the following communities of interest: defense; first responder (law enforcement, fire, emergency medical services); intelligence; science, technology, and industry; critical infrastructure; and legal. The discussion addressed the various benefits and threats of unmanned aircraft systems and ways in which this evolving technology is being integrated into the daily operations of various industries. The key takeaways from that discussion will be published soon in a special report.

Catherine L. Feinman, M.A., joined Team DomPrep in January 2010. She has 30 years of publishing experience and currently serves as editor-in-chief of the DomPrep Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and resilience communities. She also volunteers as an emergency medical technician, firefighter, and member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance's Electro-Magnetic Pulse Special Interest Group). She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Protecting the Homeland From Nefarious Drone Use

By Richard Schoeberl & Kendall J. Smith

Rezwan Ferdaus, a U.S. citizen and graduate of Northeastern University, was arrested by the Federal Bureau of Investigation (FBI) in 2011 for supporting al-Qaida and plotting to fly a motorized airplane – loaded with explosives and controlled by a global positioning system (GPS) – into the U.S. Capitol Building and the Pentagon. Though the FBI insists the public was "never in danger," the threat of a terrorist attack via unmanned aircraft system (UAS) technology is increasing. If someone other than FBI undercover agents supplied explosives to Ferdaus, the story would have been very different.

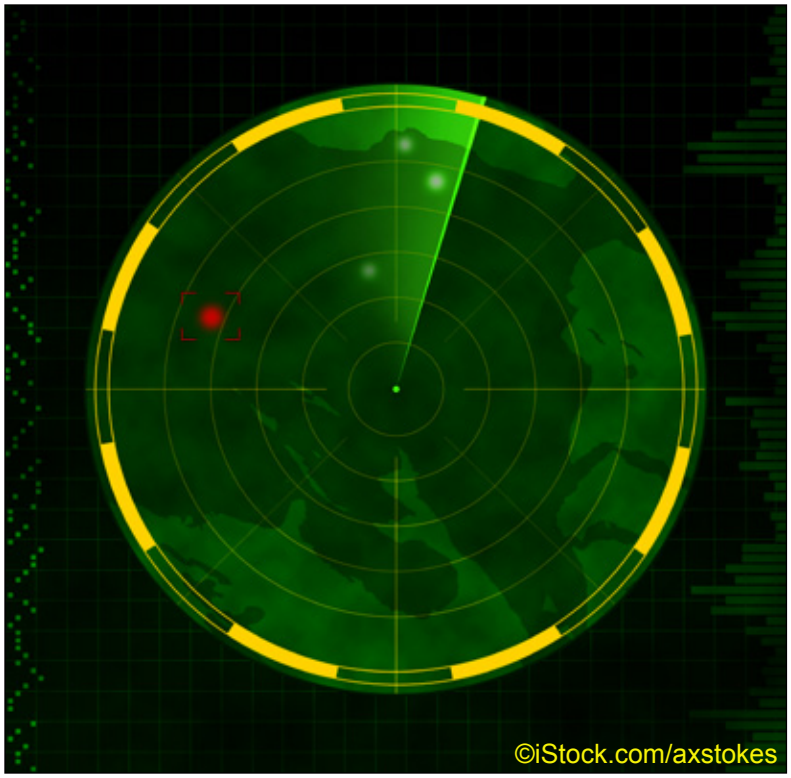
A UAS (commonly known as "drones") refers to an unmanned aerial vehicle (UAV) as well as the operating system controlling the UAV from the ground. According to a research firm report, published on 28 December 2016, total UAS sales surged to 2.2 million worldwide in 2016, and an estimated 3 million UAS will be produced and sold in 2017. The numbers are concerning, with continued and increased use of UAS by the Islamic State group (IS) abroad. The U.S. intelligence community speculates whether the United States is prepared to defend against a UAS terrorist attack on U.S. soil.

Defining the Threat

Following the online release of 13 volumes of the IS's magazine *Rumiya*, the world has begun witnessing terrorist attacks inspired by instructions detailed in that magazine. *Rumiya*, used for IS propaganda and recruitment purposes, serves as a tutorial for conducting attacks – from knife-wielding to acquisition and use of the perfect vehicle for striking crowds. IS also promotes through its online platform UAS tutorials, including how to arm an attacker with explosives. A UAS attack reduces would-be terrorists' limitations when using trucks and vehicles against hardened targets. The question is, "How prepared is the United States to defend against an object that is easily acquired without suspicion, inexpensive, portable, and provides those instructed – or inspired by the IS – a distinct tactical advantage?"

National Counterterrorism Center Director Nicholas Rasmussen told the U.S. Senate Committee on Homeland Security and Government Affairs in September 2017 that, "two years ago [a terrorist threat using UAS on U.S. soil] was not a problem, a year ago this was an emerging problem, now it's a real problem." At the same Senate Committee meeting, FBI Director Christopher Wray told members of the Senate Homeland Security and Government Affairs Committee that intelligence indicates a strong terrorist interest in using UAS technology.

Wray further commented that, "We've seen that overseas already with growing frequency. I think the expectation is that it's coming here imminently. I think they are relatively easy to acquire, relatively easy to operate, and quite difficult to disrupt and monitor." The



accessibility and affordability of UAS make it an increased concern. The IS had been using UAS since early 2014 to gather intelligence on the battlefield and broadcast videos online to further its propaganda platform. Since 9/11, dozens of bombing attacks using UAS have occurred.

According to the Federal Aviation Administration (FAA), nearly 700,000 UAS were registered over the past year, as the FAA requires individuals owning UAS weighing more than 0.55 lbs. but less than 55 lbs. to register before operating the UAS outdoors. The growing "off the shelf" commercial UAS industry has made the technology easily accessible and affordable to millions worldwide. Commercial UAS offer ready-to-fly small UAS (SUAS) with high-quality live video transmission, GPS auto-return home, 3- to 4-km range, and 25-minute flight times out of the box for less than $1,000. High-end commercial UAS (~$3,000) can lift between 6.5-13 lbs. and, depending on payload, fly 18-35 minutes. Also, for less than $1,000, custom-built UAS designed for heavy lifting could easily exceed the capabilities of hobbyist and aerial photography UAS from parts sourced online.

In a January 2017 article, FAA Chief Administrator Michael Huerta estimated that 7 million UAS could be sold in the United States before 2020. Given the number sold and required to register to the FAA, there clearly is a gap of unknown possession of this technology making it harder for law enforcement to detect owners and locations. In addition, users can purchase components to assemble or buy the entire UAS unit online under complete anonymity.

Determining Implications & Countermeasures

Implications exist for utilizing this technology to conduct an explosive or biological attack on both hard and soft targets. IS is technologically savvy and directs likeminded people to either direct or inspire such attacks. Several reasons make this a more plausible threat now than ever before:

- Operators of this technology can be out of line of sight and miles away, allowing for more covert operations;

- UAS technology use can avoid the typical and conventional security measures in place to deter terrorist acts;
- Low relative costs allow for disposable technology;
- The devices are quiet, which slows reaction time and detection;
- Many UAVs are equipped with cameras, which is in line with the IS propaganda platform; and
- Minimal piloting skills are required to operate this technology.

Several countermeasures are needed to combat this imminent threat. In August 2017, the Pentagon approved a policy allowing U.S. military bases to disable or destroy UAS that pose a potential threat. In May 2017, the Trump Administration proposed legislation (not yet approved) to expand the power to track, monitor, and destroy UAS to "any member of the Armed Forces, a federal officer, employee, agent, or contractor, or any other individual that is designated by the head of a department or agency." Law enforcement agencies and the intelligence community need systems in place that effectively detect and, when necessary, stop UAS from reaching their potential targets.

Technology has both good and nefarious uses. As UAS technology advances, the likelihood of IS (or those inspired by its ideology) using this technology becomes more likely. Beginning in February 2016, the FAA has researched UAS detection technology such as thermal cameras, as well as acoustic, radio, and radar technologies, to explore ways to best detect rogue UAS at airports. However, none of these technologies offer a "perfect" solution as they all have their limitations and many remain untested.

Overcoming Challenges

The first obstacle to overcome is detecting the presence of UAS operations and then accurately locating the UAV. The FAA is working with various private technology companies, government agencies, and universities to solve this problem.

Texas A&M in partnership with Gryphon Sensors developed an active UAS detection system comprised of ground-based sensors and radars, combining fixed sites that are being used at Griffiss International Airport in Rome, New York. This unmanned traffic management system dubbed *Skylight*, has been tested with cooperation from the New York state Governor Andrew M. Cuomo, who is investing as much as $30 million in state funding toward UAS detection, management, and innovation. The mobile version of the *Skylight* system resembles a news van with off-road and technological capabilities, highlighting a significant disparity between the cost to own and operate UAS (less than $3,000) and the cost to detect rogue UAS (hundreds of thousands to millions of dollars for research, development, and implementation).

The required equipment to defend against small, yet effective, delivery vehicles is complex to build, maintain, and operate. However, the development of mobile detection capabilities is important for deploying on short notice to locations where expensive fixed UAS detection and

management systems are not yet implemented, or to supplement defenses while more robust, fixed sites are constructed. The need for effective, accurate UAS detection and management systems is critical to support military, law enforcement, humanitarian efforts, search and rescue missions, critical infrastructure such as power plants, and general property defense.

Once located, there are several approaches for denying undesired UAS operations: physical destruction (firearms), disabling the UAS (casting nets), disrupting the wireless control or jamming GPS signal receivers, or remotely hacking the flight control software. A UAS's proximity to people or valuable resources determines the necessary actions.

If a suspect UAV is carrying potentially hazardous cargo, forcing down the UAS with kinetic measures may not be the most prudent solution. In this instance, a protocol manipulation system can passively detect and analyze radio frequency signals transmitting on unlicensed frequencies. With this information, the system can then exploit the weaknesses in the detect-control protocol to control the UAV. Combining this technology with a kinetic mechanism offers flexibility with a multitier defense system. For example, navigate the UAV to a safe location, then disable it. A potential problem with this system though is its use of common commercial UAS control protocols, which may not consider a wide variety of custom and open-source flight control solutions.

The FAA is working with various stakeholders to solve problems related to detection and identification UAS technologies.

Signal jamming and directional radio frequency interference are two more methods of denying UAS operations. Jamming GPS/Global Navigation Satellite System (GLONASS) reception can force a UAV to land using built-in failsafe mechanisms. The failsafe mechanisms address contingencies such as loss of GPS/GLONASS satellite reception, loss of radio control link, and low battery. Loss of satellite navigation could degrade the UAV and its ability to automatically hover over a specific location, making the drone more difficult to control. Loss of the radio control link would likely cause the UAV to "return home," where it autonomously returns to a predetermined location. Commercial drones often have several low-battery conditions that are intended to save inexperienced users from crashing their expensive equipment. A low battery may cause a UAV to "return home" if it has enough power. If the battery reaches a critical state where it does not have sufficient power to return home, it could trigger "auto-land," where the UAV would simply land wherever it is. To land the UAV, a combination of sensors assesses altitude and position via barometric pressure, ultrasonic sensors, and optical flow sensors.

Identifying Caveats & Future Efforts

Denying GPS/GLONASS may not be effective for two reasons: (1) not all UAS rely on satellite navigation; and (2) a moderately skilled operator could successfully execute a

mission using manual controls with visual navigation via live feed. Triggering only one of the failsafe mechanisms could cause the UAV to land in an undesirable location, so using a sequence of signal jamming techniques offers more solutions. Following is an example of an approach to multitier denial:

- Jam the radio control and video transmission links, causing the UAV to trigger the "return home" failsafe;
- Once the UAV is determined to be a safe distance away,
- Jam GPS/GLONASS, causing the UAV to stop the "return home" function and it will just hover (note: the UAV will drift with the wind);
- One could then disable the UAV with kinetic means or force the UAV to run itself to a critical battery state, causing it to auto-land.

The potential drawbacks of any singular denial method highlight that a multitier defense strategy would stand a higher chance of success against a wider variety of UAS types and attack scenarios.

Advancement is needed in detection technology to deter these attacks and assist law enforcement, but it will not eliminate the threat or the likelihood that attacks will happen. Similar to the many lone-wolf threats that go undetected, it is likely the UAS threat will increase in probability given the relative ease for acquiring and operating, as well as the difficultly for disrupting and monitoring this evolving technology.

The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the U.S. government.

Richard Schoeberl, a Ph.D. candidate (ABD) in terrorism, has over 22 years of security and law enforcement experience, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency's National Counterterrorism Center (NCTC). He has served at a variety of positions throughout his career, ranging from supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before his managerial duties at these organizations, he worked as a special agent investigating violent crime, international terrorism, terrorist financing, cyberterrorism, and organized drugs. He also was assigned numerous collateral duties during his FBI tour – including a certified instructor and member of the agency's SWAT program. In addition to the FBI and NCTC, he is an author and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, Al Hurra, and Sky News in Europe. Additionally, he has authored numerous articles on terrorism and security.

Captain Kendall J. Smith (pictured above) is currently an instructor combat systems officer 451st FTS, Pensacola NAS, Florida. He also is the director of the self-protection phase of training for undergraduate combat systems officer training (UCT). He commissioned in 2008 at Marquette University with a bachelor's degree in computer science and is currently a Master's of Science in technology management candidate. His first assignment was Randolph Air Force Base (AFB) for UCT. He joined his first operational squadron as a B-52H weapons systems officer in 96th Bomb Squadron, 2nd Bomb Wing, Barksdale AFB. He upgraded to senior weapons system officer and deployed with the 96th Bomb Squadron twice to support the Continuous Bomber Presence in the USAF Pacific Command. After two years of instructing at Pensacola NAS, he deployed to Djibouti Africa for six months as the chief of scheduling for air operations on the Combined Joint Task Force – Horn of Africa, where he earned a Joint Service Commendation Medal for his exceptionally meritorious service.

Our commitment to BioDefense

has allowed us to be ready

for the Ebola outbreak

in West Africa.

Now, with the FilmArray system

and our reliable BioThreat Panel,

we are able to test for 16

of the worlds deadly

biothreat pathogens

all in an hour.

Now That's Innovation!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com

Critical Infrastructure Partnerships – Prioritizing Assets

By Christopher Ryan

A key early step for critical infrastructure protection (CIP) programs is to identify and prioritize the most important facilities and assets for maintaining community safety, normalcy, and quality of life. Within single jurisdictions, CIP program managers typically choose prioritization criteria to determine the most critical assets. However, developing customized prioritization criteria for multiple, closely interconnected jurisdictions in the National Capital Region (NCR) – where public safety authority is decentralized – recently proved much more challenging. Here is how they overcame this challenge.

To build a regional program, representatives of each existing jurisdictional program – despite already selecting a prioritization methodology for their own use – sought to develop a new, consensus methodology that each would use voluntarily for regional assessments. Each jurisdiction's existing prioritization system for internal use would remain unchanged. A robust consensus methodology was essential to developing a regional public safety perspective that reflects the region's unusually high interdependence and joint responsibility for supporting the federal government's broad geographical footprint, but there were no known methods of developing such a consensus.

From 2016 to 2017, the NCR's Critical Infrastructure Protection Work Group (CIP WG) successfully developed regional critical infrastructure prioritization criteria by utilizing a carefully controlled, discussion-based process of trial and error in which the group applied a small set of selected assets to several existing sets of criteria. The CIP WG's success in developing consensus on regional prioritization criteria is a compelling case study in how highly interconnected, multijurisdictional regions can adopt a more holistic approach to CIP.

The Purpose of Prioritizing Critical Infrastructure Assets in the National Capital Region

The need for a multijurisdictional, holistic critical infrastructure (CI) prioritization methodology in the NCR stems from the region's unusually comprehensive interdependence and joint responsibility for supporting the federal government's broad footprint. NCR jurisdictions share critical transportation networks, drinking water supplies, communications systems, and energy resources. From a public safety perspective, the region jointly manages and shares data from license plate readers, syndromic surveillance, and automated fingerprint collection programs; closed circuit television feeds for real-time intelligence; and emergency planning, training, exercising, and incident management resources. Several jurisdictions utilize mutual aid for fire and emergency medical services every day, and even allow dispatchers to deploy first responders from other jurisdictions. Regional CI prioritization reflects that, as a practical matter, each NCR jurisdiction shares responsibility for maintaining public safety, normalcy, and quality of life in the region as a whole. Moreover, regional CI prioritization reflects that the same regional assets and partnerships provide essential services that allow the federal government's central hub to function as usual.

To develop the necessary regional consensus, the CIP WG developed an innovative workshop-based process that relied on facilitated discussion to identify the specific characteristics that make assets critical. The CIP WG's full membership was invited to participate in each workshop to ensure that the final product would reflect the region's diverse stakeholders and perspectives. Workshops included substantive contributions from: emergency management and/or homeland security experts representing Montgomery County, Maryland; the State of Maryland; Arlington County, Virginia; the Commonwealth of Virginia; the District of Columbia; the Department of Homeland Security; Joint Force Headquarters – National Capital Region, the District of Columbia Water and Sewer Authority; the Metropolitan Washington Council of Governments (COG); and University of Maryland Center for Health and Homeland Security (CHHS). Analysts from intelligence fusion centers in Maryland, the District of Columbia, and Virginia also made key contributions. Each workshop included approximately 15 to 20 participants.

Analysis of Existing Prioritization Systems

As background research, support staff from the COG and CHHS identified three existing prioritization systems to help brainstorm different kinds of legitimate criteria. All three systems considered key issues relating to asset criticality as well as the severity of specific impacts that would result from damage to or destruction of a CI asset. When used to examine CI assets, all three systems also generate a three-tiered prioritized asset list.

Criteria A examined nine possible impacts, Criteria B considered five potential impacts, and Criteria C assessed eight potential impacts. Combined, the three systems considered the following 13 impacts:

- Economic impact
- Fatalities
- Impact on national security and/or public safety
- Length of mass evacuation
- Percentage of population significantly affected
- Public Confidence/Morale
- Impact on other assets in the same CI sector
- Impact on assets in other CI sectors
- Environmental impact
- Lifeline sector status (Water, Energy, Transportation, Communications, and Emergency Services)
- Redundancy
- Hazardous/CBRNE materials status
- Cyber-dependency

COG and CHHS also constructed a "Straw Man" prioritization system not as a formal policy suggestion, but to help stimulate discussion and compel group members to think about the challenges of designing new criteria. The Straw Man includes all 13 impacts, and is based on

a combination of the other three systems and educated guesses about which characteristics would establish the most useful distinctions for regional stakeholders.

The group held an initial half-day work session in August 2016 to apply all four systems to a sample group of assets that reflect different sectors, are geographically dispersed, and appeared likely to possess varying regional criticality. The assets are listed below:

- 14th Street Bridge Complex
- Brighton Dam
- Montgomery County Government Complex
- Metropolitan Washington Council of Governments Building
- New Carrollton (WMATA/Amtrak) Rail Station
- District of Columbia Office of Unified Communications
- Reagan National Airport
- Reston Town Center
- Springfield Interchange (I-95, I-395, I-495)
- Washington Aqueduct – Dalecarlia Water Treatment Plant

After applying each system to all 10 assets, the group analyzed each set of results to identify strengths and weaknesses of the prioritization systems and pinpoint the characteristics that would provide the most useful regional findings.

Workshop Guidelines & Assumptions

Though projecting how an incident would influence CI assets may seem straightforward, the group quickly realized that the analysis depended largely on the nature of the events that would damage or destroy the asset. For example, an attack on a large airport could result in a major fuel spill, or might have a less significant environmental impact. The same attack could moderately damage the airport, or destroy it. Applying the systems to each asset was difficult without additional context.

To guarantee comparable results between the four systems, and to make sure the new regional system could be used for all hazards and all 16 CI sectors, the group agreed that discussion would incorporate the related principles of "generic total loss" and "non-scenario based" analysis. A generic total loss is a hypothetical state in which an asset that is functioning under normal conditions is assumed to have disappeared along with the people and property the asset contained at the time of disappearance. Everything that asset was doing would halt and the asset would need to be rebuilt. The generic total loss approach thus added the context that the group needed by basing the analysis on consistent points of reference, allowing the group to focus on the potential impacts of an asset loss rather than the scenario-specific details of how an asset might be damaged or destroyed.

Additional ambiguity remained concerning the fatality and economic impacts. The group agreed that fatalities would be determined based on the maximum capacity of each asset under normal circumstances. Economic loss totals would include the cost of rebuilding each asset as well as the total value of lost economic activity resulting from each asset's absence.

The group also agreed to make all decisions based on consensus. Though complicating matters somewhat by not relying on a formal decision-making process, the group recognized that each partner in the room was voluntarily agreeing to work regionally, and would only continue to do so if every partner agreed that the prioritization system was legitimate. To ensure that partners would be able to agree to the new system's legitimacy, it was essential they felt their concerns were fully incorporated into the decision-making process.

Finally, the group agreed to rely on the collective's best professional judgment to apply the criteria, even though they would not have immediate access to all of the information they would need to confirm each judgment. Since the group regarded the workshop as the start of a long-term, iterative process of evaluation and reevaluation, they agreed to conduct follow-up research as needed after the workshop and reexamine assets as appropriate.

Sample Findings

Each of the four existing prioritization systems generated three separate tiers of prioritized assets. To be consistent with the Department of Homeland Security's two-tiered national prioritization system (Levels 1 and 2), the group agreed to refer to each of the four systems' highest impact severity tiers as Level 3, middle tiers as Level 4, and lowest tiers as Level 5.

After the group agreed to the ground rules, they then held informal, roundtable discussions to determine whether a generic total loss of each asset reached Level 3, 4, or 5 severity thresholds for each impact within each of the four systems. Though the group will not disclose the four systems they examined due to security concerns, Table 1 provides a real-world example of differences in impact severity thresholds that are typical for the four prioritization systems the group considered during the workshop.

Harris County, Texas Critical Infrastructure Prioritization Criteria			
	Level 3	**Level 4**	**Level 5**
Fatalities	Greater than 1,000 prompt fatalities	Greater than 100 prompt fatalities	0-100 prompt fatalities
Length of Mass Evacuation	Mass evacuations with a prolonged absence of greater than 3 weeks	Mass evacuations with a prolonged absence of more than 2 weeks	Mass evacuations (100s to 1000s) with a prolonged absence of more than one week
Economic impact	Greater than $1 billion in first-year economic consequencs	Greater than $100 million in first-year economic consequences	$0-$99,999 first-year economic consequences

Table 1. Examples of Impact Severity Thresholds

Table 2 shows the impact severity thresholds that the group determined applied best to one asset, which the group chose not to identify due to security concerns. Blacked out portions of the table indicate impacts that the corresponding prioritization system does not examine. "Unranked" indicates that the asset did not meet the lowest severity threshold for that impact.

Asset 1 – Criteria Thresholds Met				
Impacts	**Criteria A**	**Criteria B**	**Criteria C**	**Straw Man**
Economic	Level 5	Level 3	Level 3	Level 3
Fatalities	Level 4	Level 3	Level 3	Level 3
National Security/ Public Safety			Level 4	Level 4
Length of Mass Evacuation		Unranked	Unranked	Unranked
% of Population Affected	Level 5	Level 3		Level 3
Public Confidence/Morale		Level 4	Level 3	Level 3
Impact on Assets/ Facilities/Systems within Individual Sector	Level 3	Level 3		Level 3
Mission Impact on Other CI Sector Assets/Facilities	Level 5	Level 5		Level 5
Environmental	Level 3	Level 3		Level 3
Lifeline CI Sector	Level 3			Level 3
Redundancy	Level 3			Level 4
CBRNE/Hazmat	Level 5			Level 5
Cyber				Level 3

Table 2. Criteria Thresholds Met – Asset 1

Selecting Impacts

After applying the four systems to all 10 assets, group members worked independently to review the results in detail and develop an opinion of which impacts were most important to include in a regional system. When the group reconvened for a second half-day session the following month, they moved through the list of impacts and asked, by a show of hands, which impacts should be included in an NCR prioritization system. Clear consensus emerged for 11 of the 13 impacts – the group was nearly unanimous that eight of the impacts should be included, and three others should be excluded. After discussing the two remaining impacts, the group agreed that the NCR's CI prioritization criteria would examine the following impacts:

- Lifeline Sector
- Fatalities
- National Security/Public Safety
- Percentage of Population Affected
- Impact on Assets/Facilities/Systems Within Individual Sector
- Mission Impact on Other CI Sector/Assets/Facilities
- Economic Impact
- Cyber-Dependent
- Length of Mass Evacuation

Selecting Thresholds

Having decided on which impacts to include, discussion transitioned to the question of which of the four existing systems' impact severity thresholds would be best for the NCR criteria. Initial discussion revealed broad group consensus that the Straw Man's thresholds did the best job of identifying meaningful similarities and dissimilarities in the projected impacts of a generic total asset loss. Rather than suggesting changes to the Straw Man's thresholds based on educated guesses, the group agreed to keep the existing language and revisit the discussion once the group had used the regional criteria. Group members could then suggest specific changes based on experience.

Conclusion

The CIP WG utilized a carefully controlled, discussion-based process of trial and error to develop a three-tiered regional CI prioritization methodology. The new criteria work better for the NCR than other prioritization systems because they focus on consequences that pose the greatest degree of concern to the region's subject-matter experts, and because the criteria are customized to reflect the NCR's unique interconnectedness and shared responsibility for public safety. The CIP WG's success in developing a consensus regional prioritization criteria is a compelling case study in how highly interconnected, multijurisdictional regions can adopt a more holistic approach to critical infrastructure protection.

A subsequent article on this topic will examine how the NCR's CIP WG synthesized information about the impact severity thresholds that each asset met into a weighted, numerical scoring system. With the numerical scoring system in place, the CIP WG is able to build, maintain, and update a single, prioritized regional list of CI assets that they can use for all hazards and all 16 sectors.

Christopher Ryan is a senior policy analyst with the University of Maryland's Center for Health and Homeland Security (CHHS). Since joining CHHS in 2015, he has focused primarily on providing technical assistance to the National Capital Region on critical infrastructure protection, complex coordinated attack preparedness, strategic planning, program management, capabilities assessment, and grant management. He previously worked as a Homeland Security StateStat analyst in the Maryland Governor's Office, where he provided policy and programmatic guidance to state agencies and tracked their progress toward statewide goals. He also represented the Governor's Office on the interagency Ebola Planning Cell. He holds a bachelor's degree in history from Towson University and a master's degree in history and public policy from The George Washington University.

Freight Rail Safety and Emergency Management

By Kay C. Goss

During the second week of October 2017, the DomPrep Journal hosted and Draeger sponsored a series of presentations and discussions, which included most of the major federal agencies engaged in freight rail safety and security, as well as the American Association of Railroads. To add to that discussion, several states have made significant contributions to freight rail safety. Three major state and local emergency management agencies that have made these major strides in rail safety and security are described here.

The states of Minnesota, Washington, and California have developed programs and taken actions to enhance public safety and emergency management for the freight rail infrastructure, integral to their communities and surrounding areas.

Minnesota Department of Public Safety's Homeland Security & Emergency Management Division

Under Governor Mark Dayton, Tenzin Dolkar serves as Minnesota's state freight rail director, leading the state's efforts to enhance railway safety and to ensure safe and efficient rail operations through: infrastructure improvements; first responder training and support; monitoring of rail movements; and coordination with community stakeholders and railroad companies. To help with funding for emergency response and preparedness training, Minnesota Department of Public Safety's Homeland Security and Emergency Management (HSEM) Division has a Railroad and Pipeline Safety Account for interested communities.

Rail incidents, involving crude oil, that have occurred in nearby states have raised additional safety concerns in Minnesota. To address these concerns, Dayton signed legislation in July 2014 requiring the Minnesota Department of Public Safety to provide statewide oil transportation awareness training to local jurisdictions. As of 12 October 2017, HSEM's efforts include the following:

- 6,201 first responders from 210 departments and agencies trained to better understand and protect against hazards related to the transport of oil and other hazardous substances (with 296 sessions held and more scheduled for the future);
- Three tabletop exercises related to oil transportation, with participants receiving jurisdictional maps highlighting key community assets located within a half mile of the rail line;
- Advanced training related to crude oil response for all state Chemical Assessment and Emergency Response Teams;
- 1,533 first responders from 66 departments and agencies have completed the higher operational training level, with 86 sessions conducted and five approved training providers; and

- The formation of an oil training advisory group comprised of the Minnesota Department of Public Safety, Minnesota Pollution Control Agency, and Minnesota Board of Firefighter Training and Education.

HSEM completed its report outlining the state's response capabilities for an oil transportation incident, which includes emergency preparedness, first responder training, and best practice recommendations. Other legislation protects communities through which railways carry crude oil and other hazardous materials by promoting: increased oversight of railroad companies; more railway inspection requirements; and better emergency response training and preparedness across the state.

The Department of Public Safety's HSEM is actively involved in many activities to improve the safety and security of freight rail movement. HSEM works with railroad and pipeline companies to develop safety protocols and facilitate public-private sector coordination that enhances an understanding of oil and other hazardous substances. This department also assists local governments as they incorporate emergency response information into their emergency operations plans. These efforts include:

- Collaborating with local emergency managers and responders to understand the dangers of oil and other hazardous substances traveling by rail through their jurisdictions; and
- Partnering with the Minnesota Department of Transportation, Minnesota Pollution Control Agency, and railroads to integrate rail safety legislation.

King County, Washington, Emergency Management Office

King County is highly regarded for its overall emergency preparedness efforts and serves as one of the largest transportation hubs – with major railroad operations – in the Pacific Northwest. Freight rail safety and emergency management issues in the region include exponential growth in the number of trains carrying highly flammable crude oil and coal, which increases the risk of transportation accidents and makes the area vulnerable to various types of transportation emergencies.

To help prepare its community for potential rail threats, the King County website page on transportation accidents provides public information on rail hazards, preparedness and response actions for transportation incidents, and additional resources. Its website shares five slide presentations on freight rail safety and emergency management, which are ready for public outreach and technical training.

California Governor's Office of Emergency Services (CalOES)

In a statewide gap analysis, CalOES found that several local municipalities had created specialized hazardous material response units (hazmat teams), which are responsible for protecting their communities, public resources, the environment, and property when an incident involving hazardous materials occurs. These teams are mostly located in densely populated metropolitan areas throughout the state and vary in their capabilities. To facilitate possible expansion and ensure regional mutual aid response when needed, CalOES integrated these hazmat teams into its Standardized Emergency Management System (SEMS), National Incident Management System (NIMS), and Statewide Fire, Rescue, and Hazardous Materials Mutual Aid Plan. In addition, CalOES created a HazMat Team Typing Program to better identify and coordinate these specialized resources for emergency response.

Since 2004, the Fire and Rescue Branch of CalOES and FIRESCOPE (Firefighting Resources of California Organized for Potential Emergencies) have been certifying the state's hazmat team response competency and ensuring coordination of hazmat response teams with the State Master Mutual Aid System, in accordance with accepted FIRESCOPE mutual aid and SEMS response standards. California's system provides a coordinated and reliable mechanism for local, regional, and state authorities to leverage when additional resources, specialized capabilities, and multijurisdictional responses are needed following a major hazmat incident. Four significant objectives drive this system:

- Requirements for standardized and certified training;
- Development and sustainment of a standardized Hazardous Materials Equipment List (based on performance typing standard);
- Development of the HazMat Team Typing concept (based on intervention/response capability); and
- On-site inspections of hazmat teams for compliance, certification, and standardization.

As of March 2015, CalOES had certified 60 hazmat teams that voluntarily entered the HazMat Team Typing Program. However, gap analysis reflects that qualified hazmat teams throughout rural California are still lacking. To address this gap, CalOES strives to enhance its emergency hazmat response capabilities, which includes response times, equipment, new and refresher responder training, and additional resources. Adding to the challenge in California, around 32% of its 56,000 firefighters are assigned for sustainment of critical hazmat response and recovery capabilities and resources to ensure rural rail safety.

States and local governments contribute significantly to freight rail safety and work with federal agencies, particularly US DOT in the Operation Lifesaver Program and share best practices with each other and programs for each of their surrounding communities.

Kay C. Goss, CEM®, is president of World Disaster Management, U.S. president of The International Emergency Management Society, president of the Council on Accreditation of Emergency Management Education. She is also part-time faculty online and Go-To-Meeting, as well as in person, in the Executive Master's Program in Crisis and Emergency Management at the University of Nevada at Las Vegas and in the Graduate Program in Emergency Management and Homeland Security at Metropolitan College of New York. Previous positions include: executive in residence at the University of Arkansas; senior principal and senior advisor of emergency management and continuity programs at SRA International (2007-2011); senior advisor of emergency management, homeland security, and business security at Electronic Data Systems (2001-2007); associate Federal Emergency Management Agency director in charge of national preparedness, training, and exercises, appointed by President William Jefferson Clinton and confirmed unanimously by the U.S. Senate (1993-2001); senior assistant to the governor for intergovernmental relations, Governor William Jefferson Clinton (1982-1993); chief deputy state auditor at the Arkansas State Capitol (1981-1982); project director at the Association of Arkansas Counties (1979-1981); research director at the Arkansas State Constitutional Convention, Arkansas State Capitol (1979); project director of the Educational Finance Study Commission, Arkansas General Assembly, Arkansas State Capitol (1977-1979).

Invisible Threats Exposed

AP4C

Portable Chemical Detection System
Protects First Responders, Military & Infrastructure

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport

Learn More Online

PROENGIN

Chemical and Biological Detection Systems

Chemical Attack on Public Transport – A Likely Scenario

By Zamawang Almemar

Some experts say that a chemical attack plot on Western public transportation systems such as this one is inevitable: It is 0753 on a Tuesday morning at the busy red line subway station in Washington, D.C. The Islamic State group (IS) just claimed responsibility for a chemical attack that took place there by three IS supporters (two males and one female) about half past the hour. The Metrorail transportation staff and first responders are rushing to care for the victims of what seems to be a sulfur mustard attack.

This is a highly likely scenario according to some experts in the field of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) preparedness and response. This scenario is feared in the United States and seems to be an imminent threat in Europe. In late October 2017, IntelNews.org stated that the German newspaper Die Welt reported that spies warned European security services of "a possible terrorist attack by the Islamic State using chemical weapons." They were warned that the Sunni militant group might assemble improvised explosive devices (IEDs) using chemicals or toxic gasses. This comes at a critical time as members of the IS head home to their residences in both Europe and the United States.

Reports of the scenario cautioned by the European intelligence agencies should not be underestimated. Such plots are plausible, as was the plot Australian authorities foiled in early August 2017. In that case, CNN reported that two brothers living in Sydney had received IED parts and instructions from a senior IS commander to detonate an explosive on a plane and disseminate a toxic hydrogen sulfide chemical at a public location in Australia.

A Westward Shift for Chemical Threats

As IS continues to lose control of territory in Iraq and Syria, supporters increasingly resort to unconventional means of causing mass disruption. In an interview published on 25 October 2017, Lt. Gen. Paul E. Funk II, the U.S. commander of the international military campaign against IS told the *New York Times* that the terror group currently only controls 5% of territory than it did in Iraq and Syria three years earlier. These claims are to be taken seriously. As the terror group loses physical ground, the West continues to witness a substantial increase in unconventional terror threats by IS through knife attacks and vehicle ramming incidents.

These unconventional means for IS to cause mass terror are only expected to rise as thousands of foreign fighters return home. According to The Soufan Center, a U.S.-based think tank, at least 5,600 IS supporters have returned home (spanning 33 nations) over the past two years as the group loses territory in Iraq and Syria. These findings come as the result of the liberation of Raqqa – the terror group's de-facto capital for three years – by the U.S.-led Syrian Democratic Forces (SDF). In Raqqa, the Syrian Democratic Forces had uncovered the names of thousands of registered foreign fighters who had joined IS from over 100 different countries, the BBC News reported.

The use of chemical weapons is reprehensible, and the general population who are in direct line of these attacks should be protected. As outlined by the Organization for the Prohibition of Chemical Weapons (OPCW) October 2017 report, there are many accounts of chemical weapons use by state and non-state actors against innocent civilians in both Iraq and Syria, including: the sulfur mustard attack by IS in Um-Housh; and the sarin attack by the Assad regime in Khan Sheikhoun in Syria. Given the terror group's ideology, it appears likely that IS supporters will eventually release such chemicals and toxin gasses – perhaps using drones as their delivery system – in a public location of a Western nation. The use of chemical weapons represents not only a physical threat, but also an act of psychological terrorism.

Never Underestimate the Enemy

In Issue 15 of the Dabiq magazine, IS calls on its jihadists to keep their operations "simple and effective," use a weapon to "cause the most damage and panic," and "terrify the disbelievers in their homelands." Similarly, in Issue 9 of its more recent Rumiyah magazine, IS encourages supporters to lure innocent victims such as college students into their apartments by posting false "For Rent" signs with a contact number, then slaughtering and dismembering them. This is supplemented with their propaganda about using heavyweight trucks to crash into large crowds, thus causing the most casualties. People in the West live in uncertain times with an unpredictably dangerous enemy and a significant amount of threats.

It is important to document the urgency of public and domestic preparedness and provide proper training to first responders and local authorities as the first line of defense in resisting such attacks. Readiness is key when the unthinkable happens, and being prepared not only for responding to a toxic chemical incident, such as the scenario sketched earlier, but also having the proper tools to prevent these types of incidents from ever taking place. Such efforts are easier said than done, but they begin with the public being vigilant and reporting on unusual activities within their vicinities. Reporting anomalies and suspicious activities to local authorities ultimately saves lives and maintains homeland security.

Zamawang F. Almemar is a senior chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) and non-conventional threat consultant. She is directly involved in counterterrorism efforts that specifically deal with acquisition and manufacturing of chemical and biological weapons, as well as improvised explosive devices. She is finishing her third masters degree in biodefense at George Mason University with emphasis on global terrorism and their use and acquisition of CBRNE threats to national security. She was born and raised in Sulaimanyiah, Iraqi Kurdistan during the Iran-Iraq war. She fled the atrocities of the Saddam regime, seeking asylum in the United States in 1997. Since then, she has achieved two bachelor's degrees in biology and chemistry and two masters degrees in chemistry and mechanical engineering from the University of Colorado at Colorado Springs (UCCS). At UCCS, she taught graduate courses in biology and mechanical engineering and was a Ph.D. graduate fellow in mechanical engineering conducting research focused on nanobiotechnology. She has numerous publications on spreading awareness about the chemical attacks by IS on the Kurdish population in Iraq and Syria and has conducted countless seminars and briefs to senior leaders and decision makers in the United States and the international community. She recently established her own company advising on CBRNE-related issues in theater.

Staying "PRIMED" for a Radiation Event

By Grant Coffey

Chemical, biological, radiological, nuclear, and explosive (CBRNE) events are low in frequency, but high in consequence, requiring a frequent and more targeted emphasis on the way that responders train and learn. Radiation is often not well understood. It can be intimidating for both the public and for first responders. Radiation cannot be seen, smelled, or heard. Yet, risk is relatively easy to mitigate when responders have been adequately trained and equipped.

One training checklist responders can use is the acronym "PRIMED," which stands for Prepare, Recognize, Input, Monitor, Experience, and Decision.

A Six-Step Training Checklist

Prepare. Radiation events can be overwhelming and chaotic. Preparation must be done before the event and should be based on best practices. Meetings and trainings with support agencies like local state radiation regulatory agencies, Civil Support Teams, and Radiological Assistance Program teams should occur before the need arises. This sets a critical foundation in a successful working relationship: responders arriving on scene can integrate with radiation officials to work quickly and effectively. A radiation specialist from the closest hazmat response team can be an effective resource, so it is important to build rapport and cross-team familiarization with local hazardous materials response teams.

Recognize. Upon arriving on scene, responders should check-in with incident command and perform a quick situational assessment. Rushing in before recognizing hazard zones and personal protective equipment (PPE) requirements is dangerous. Basic recognition of the scene type and scope of the incident can prevent a minor scene from becoming a catastrophe. It is imperative to recognize the possibility of the presence of radiation.

Input. Identify scene "cues and clues." These are important pieces of the much larger incident picture. Ionizing radiation can be anywhere within a community. Knowing what type it is and where it is helps responders to develop a safe and effective plan. There are four basic categories of ionizing radiation: naturally occurring radioactive material, industrial, medical, and special nuclear material. Understanding where each of these types of radiation are located in the community helps responders quickly recognize anything unusual, which should raise suspicion. One key input item here is an explosion with an unidentified

source. In this case, the possibility of radiation should be suspected. Once radiation is ruled out, responders can then proceed with other scene priorities.

Monitor. Responders to a CBRNE incident must be able to assess radiation levels, verify radiation boundaries, define contamination areas, and, when possible, attempt to identify specific radionuclides. This could be a critical piece of information in the attempt to determine whether an event is accidental or intentional. It is important to remember that equipment provides only a partial assessment and is only as good as the knowledge and skill of the user.

Experience. Ultimately, the brain is the best tool in the field. Experience is vital, but should be based on tested operational truths from other events and then learned. Only then can this experience be integrated into daily response habits. This is especially critical when dealing with radioactivity because there are few incidents to learn from.

Decision. The final but perhaps most important step in the PRIMED process is making a decision. Radiation incidents, though overwhelming, have common patterns. If these patterns are recognized early, they can help pave the way to safer decision making under stress. Radiation is a predictable physical phenomenon, which can be used to a responder's advantage.

Response Checklist

Although radiation is naturally occurring energy, responders should strive to avoid any additional amount of ionizing radiation. Once it has been determined that radiation is present, responders must keep exposure or dose of radiation to a minimum by observing ALARA, which stands for "As Low As Reasonably Achievable." This term refers to radiation exposure and reminds responders to always pay attention to personal safety. ALARA is a regulatory requirement but, aside from that, ionizing radiation is still a major health and safety hazard. Without applying the principles of ALARA, a worker who is continually exposed to ionizing radiation can receive irreversible cell damage, which can manifest in harmful ways (e.g., increased risk for cancer, genetic mutations, organ failure, and even death).

Training and response checklists help responders limit exposure to and mitigate the consequences of radiological exposure during daily operations.

In addition to practicing ALARA, it is critical that first responders use appropriate PPE when responding to a radiation incident. Three factors should be considered for minimizing the effects of radiation exposure:

- *Time* – Responders should spend as little time as possible in a radiation field to minimize dose.
- *Distance* – Responders should put distance between them and the source. Further distance from a radiation source means less exposure.
- *Shielding* – Responders should wear appropriate PPE (including respiratory protection) and keep dense materials between them and the radiation field.

> Ionizing radiation exists in the form of energy (x-rays, gamma rays) and sub-atomic particles (alpha and beta particles). High-density materials such as lead and thick steel or concrete can provide some shielding from the high-energy waveform of ionizing radiation, though generally not practical on an emergency scene.

The essential point is that responders must observe ALARA during radiation events and always remember radiation rule #1: "Turn it on and put it on." A personal radiation-monitoring device (PRD) is critical to alert responders to the presence of radiation. PRDs are important tools that can save lives by alerting responders when they have entered a significant radiation field or have accumulated a significant dose of radiation. Good education and field guides based on operationally tested factors are key to helping organize on-scene priorities. Radiation safety is of the utmost importance. By following the principles from the PRIMED training checklist and heeding the protection mantra ALARA, responders can minimize their risk of radiation exposure.

Grant Coffey is a retired Portland Fire & Rescue Hazmat Team coordinator, College Fire Science instructor, and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) expert of nearly 40 years. He trains fire, police, military, and industry hazmat responders. He has National Fire Protection Association (NFPA) certifications for radiation specialist and is a state of Oregon radiation safety officer. He is also a hazmat specialist and incident safety officer and has experience in emergency management and various other CBRNE hazmat disciplines. He hosts CBRNE response training videos online at FLIR.com/PRIMED.

Biothreats – Advocating Action Through Transition

By Robert C. Hutchinson

On 15 November 2016, the President's Council of Advisors on Science and Technology (PCAST) released a letter report to the president on "Action Needed to Protect Against Biological Attack." PCAST urged the president for immediate action to ensure that the nation has the ability to meet these challenges with near-, medium-, and long-term goals. It is critical that the recommendations in this letter are conveyed to the current administration, and not lost in transition.

The letter stated that biotechnology has been growing at an exponential rate over the past several decades, with great benefits and serious potential for destructive use by both states and individuals. Released at the end of the previous administration, the letter did not permit sufficient time for meaningful action. However, it is still relevant for this and future administrations in a world of vast biotechnology and biosecurity vulnerabilities – the new landscape according to PCAST. Reportedly, PCAST has not been reauthorized or fully staffed under the new administration.

PCAST Concerns

PCAST outlined the federal government's approach to defending against biological threats over the past two decades with a review of some of the relevant congressional acts, strategies, and plans. Unfortunately, these governmental actions may not have evolved at the same rate as biological threats. Technology, research, and nature have created risks and challenges beyond previous expectations.

According to the letter, biological threats differ from nuclear or chemical threats since biologically engineered organisms require more modest resources and smaller facilities similar to an ordinary research laboratory. Beyond the challenges of locating a suspect laboratory, PCAST stated:

> *A deliberate biological attack could also differ in important ways from a naturally occurring disease outbreak or accidental release. A well-executed intentional attack could, for example, begin with near-simultaneous release of a biological agent in multiple, geographically dispersed areas to reach the greatest number of individuals as quickly as possible; moreover, a pathogen might be deliberately modified to affect its spread or to be resistant to current preparedness and response capabilities.*

Biodefense Strategy

The PCAST letter focused on five key components that must be part of a comprehensive biodefense strategy:

- Scientific analysis of the scope of the problem;
- Intelligence gathering to detect activity by potential adversaries;
- Biosurveillance to detect the presence of biothreats;

- Development of effective medical countermeasures to protect against biothreats; and
- Leadership and organization.

The next significant biothreat may not be manmade but a naturally occurring infectious disease. In the past 20 years, there has been an expanding list of global health threats, including: Severe Acute Respiratory Syndrome (SARS); Middle East Respiratory Syndrome (MERS); Ebola; Marburg; Lassa; Zika; and various influenzas such as H1N1, H3N2, H5N1, H5N6, and N7N9. Planning for such naturally occurring diseases and manmade threats often overlap and complement each other.

Even though the United States has invested billions of dollars to prepare for and respond to a biological attack or serious natural disease outbreak since the turn of the century, PCAST believes that it is necessary to rethink the overall organizational structure for anticipating, preparing for, and responding to biological threats. PCAST argues that the efforts have been distributed between various departments and federal agencies without optimal coordination, mechanisms to evaluate progress, or adequate focus on and accountability for long-term strategic goals. PCAST identified recommendations to address these concerns.

Recommendations

PCAST identified six recommendations for the president:

- The president should create a new interagency entity charged with planning, coordination, and oversight of national biodefense activities across the Intelligence Community and the Departments of Defense (DoD), Homeland Security (DHS), Health and Human Services (HHS), and Agriculture. The entity should be co-led by the assistant to the resident for homeland security and counterterrorism, the assistant to the president for science and technology, and the chair of the Domestic Policy Council.
- The president should request that Congress establish a Public Health Emergency Response Fund of at least $2 billion. The fund would support mobilization of rapid federal responses to serious, rapidly emerging natural or intentional infectious-disease events, including: public health interventions (by the Centers for Disease Control and Prevention); scientific research (by Biomedical Advanced Research and Development Authority and National Institutes of Health); regulatory activities (by the Food and Drug Administration); and global response (by DoD, Centers for Disease Control and Prevention, and the U.S. Agency for International Development).
- As part of its national biodefense strategy, the White House should act to substantially strengthen federal, state, and local public health infrastructure for disease surveillance, as well as promote a stronger international system of disease surveillance.
- The White House should set the following ambitious 10-year goals with appropriate funding (of at least $250 million per year) for medical countermeasures preparedness. The secretaries of HHS and DoD should report annually to the White House about progress and impediments to reaching these goals.

- The United States should set a national priority to identify and develop additional classes of broad-spectrum antibiotic and antiviral drugs. Building on progress already made pursuant to the president's Executive Order on Combating Antibiotic Resistant Bacteria, and the corresponding National Strategy and National Action Plan, the United States should fully implement PCAST's recommendations from its 2014 report "Combating Antibiotic Resistance" related to antibiotic development, as well as the analogous strategies for antiviral development.
- The DoD, HHS, and other government agencies should promote vigorous basic and applied research efforts in academic, industrial, and government laboratories with the goal of developing new types of countermeasures. These countermeasures should be rapidly and easily modified to target, safely and effectively, specific human-made and naturally occurring pathogens. The delivery of approved countermeasures should be within days after an agent's detection and characterization.

These recommendations are not new, but they remain critical for the nation and global public health. These concerns have been discussed and addressed by many other organizations interested in global public and economic health. Nongovernmental organizations and other private sector partners, including the World Bank, continue to support and fund the planning and preparedness for epidemics and pandemics.

World Bank Leadership

In 2016, the World Bank held its first Simulation Exercise on Pandemic Preparedness for ministers of finance from selected countries that receive funds from the International Development Association – the World Bank's fund for the poorest countries. The exercise included a discussion along with two videos depicting a fictional country in the early stages of a disease outbreak and then in the middle of a severe outbreak several months later. The ministers learned what could have been done differently to prevent the severe outbreak and their countries' levels of preparedness for the threat.

The World Bank exercised another pandemic simulation at its 2017 annual meeting. The exercise was reportedly the fourth organized by the World Bank due to the lessons learned from the response to the 2014 Ebola outbreak in West Africa. The simulation analyzed the effects on travel and tourism from an outbreak of a mysterious respiratory virus in a hypothetical country. The impacts on trade and travel – fear of economic consequences – have been two of the primary reasons nations are often reluctant to publicize outbreaks.

The International Working Group on Financing Preparedness, in coordination with the World Bank, issued "From Panic and Neglect to Investing in Health Security: Financing Pandemic Preparedness at a National Level" in 2017. The report proposes ways in which governments and development partners can finance investments in countrywide and regional preparedness and response capacities for pandemics and other health emergencies. The report identified 12 integrated and interdependent recommendations to ensure adequate and sustained preparedness financing.

In 2017, the World Bank launched specialized bonds aimed at providing financial support to the Pandemic Emergency Financing Facility, a facility created by the World Bank to channel surge funding to developing countries facing the risk of a pandemic. It is the first time World Bank bonds have been utilized to finance efforts against infectious diseases.

Calls for Action

The next global health threat may not be naturally occurring, but rather an intentional bioterrorism attack. In a February 2017 op-ed timed to coincide with his speech at the 2017 Munich Security Conference, Bill Gates made the point that a fast-moving airborne pathogen could kill more than 30 million people in less than a year. In a March 2017 cable news interview, former Senator Joseph Lieberman, the co-chair of the bipartisan Blue Ribbon Study Panel on Biodefense, expressed great concern about a group such as ISIS developing a powerful synthetic influenza and introducing it into the population.

In 2017, the House of Representatives, Committee on Homeland Security reviewed the progress made by the government since the Implementing Recommendations of the 9/11 Commission Act of 2007. In the area of biosurveillance, the committee recommended that the president should designate a high-ranking official in the White House to coordinate federal biosurveillance and biodefense efforts.

A Year Later

The PCAST letter is not the first attempt to identify the serious vulnerabilities and challenges the nation faces for manmade and naturally occurring biological threats. Nevertheless, this high-level knowledgeable group has addressed an area long ignored due to competing threats and considerable diversions.

The six recommendations provide focus and assist a concerted effort to plan and prepare for these threats before it is too late. However, this subject may not gain traction before a significant biological attack or serious pandemic in a nation that is keenly focused on nuclear proliferation, terrorism, and mass shootings. It certainly should, though, because a pandemic-causing novel infectious disease may produce more serious cascading consequences than any threat. According to Lieberman's March 2017 interview, a global pandemic could kill more people than a nuclear war.

The PCAST letter shall be added to, or lost in, the numerous reports, studies, findings, and collaborations calling for action and preparedness for a global public health threat. Although this thoughtful letter advocating action may be lost in a time of political transition due to its late issuance and competing priorities, it should not be overlooked. It is a critical subject for past and future administrations for a foreseeable danger.

Robert C. Hutchinson is a former deputy special agent in charge and acting special agent in charge with the U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement's Homeland Security Investigations in Miami, Florida. He retired in September 2016 after more than 28 years as a special agent with DHS and the legacy U.S. Customs Service. He was previously the deputy director and acting director for the agency's national emergency preparedness division and assistant director for its national firearms and tactical training division. His writings, interviews and presentations often address the important need for cooperation, coordination and collaboration between the fields of public health, emergency management and law enforcement. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.

EMERGENCY SERVICES WEBINAR SERIES 2017

KNOWLEDGE WHEN YOU NEED TO RESPOND

In the world of emergency operations, conditions change. So does the knowledge needed to respond effectively. American Military University (AMU) is proud to host a series of free, 1-hour webinars for responders and emergency managers, covering these and other essential topics:

- Violent Incident Consequence Management, the Emergency Manager's Role
- Principal Investigator for the Firefighter Injury Research and Safety Trends (FIRST)
- Drafting and Implementing Effective Fire Department Policies and Procedures
- Financial Systems Management for Fire and EMS Agencies
- Organized Response to Mass Casualty
- Firefighter Health: Heart Healthy Solutions

Webinar attendees may receive a 5% tuition grant for degree and certificate courses at AMU.

REGISTER FOR THE WEBINAR SERIES TODAY AT
PUBLICSAFETYATAMU.COM/ DPJ

FOR MORE INFORMATION ABOUT CUSTOMIZED TRAINING TO MEET YOUR NEEDS, CONTACT ANTHONY MANGERI AT
AMANGERI@APUS.EDU.

AMU American Military University
Learn from the leader.™

AMU is part of the accredited American Public University System and certified to operate by SCHEV.