domestic preparedness .com

DomPrep Journal

Subscribe

Volume 12, Issue 12, December 2016

Yet To Come

Since 1998, Critical Information for Preparedness and Resilience

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

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

Kerri Kline
Project Manager
kkline@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

American Military University

BioFire Defense

FLIR Systems Inc.

PROENGIN Inc.

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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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.

Featured in This Issue

About the Cover: December is the time to reflect on the past, contemplate the present, and forecast what is yet to come. The year 2016 was full of surprises that could change the course of 2017, but emergency preparedness and resilience professionals are ready for the challenge. (Source: ©iStock.com/doomu)

Editorial Remarks

By Catherine L. Feinman

This past year has had some unexpected twists and turns as the political and social climates shifted, terrorist tactics changed, new diseases emerged, and many questions about what is "Yet to Come" have been raised. To answer some of these questions, DomPrep asked subject matter experts to forecast some of the hot topics in emergency preparedness and resilience for 2017. Leading the issue is DomPrep Publisher Martin Masiuk's reflection on the past, present, and future of DomPrep.

Christopher Milburn then addresses the political and social environment, with the U.S. presidential elections spurring discussion about the role of authoritarianism and the domestic and international challenges and threats the next administration will face. Richard Schoeberl follows by emphasizing that bombs cannot stop a religion, belief, or ideology. When combating terrorism, leaders must consider the physical, psychological, and financial implications of their decisions and actions in order to plan effectively.

Emergency preparedness strategies for potential threats may include technology, healthcare plans, and government programs that factor in flexibility to address the future unknowns. For example, Darren Price shows how use of unmanned aircraft systems can be expanded for emergency management applications; Robert Hutchinson describes the need for an ever-changing biothreat readiness plan; and Jeffrey Kaliner explains the need to start with a solid foundation of guiding principles to maintain core capabilities as new threats emerge.

Of course, fortifying the nation's infrastructure is a step in the right direction toward mitigating future threats. J. Michael Barrett wants to "Make the Grid Great Again" by encouraging investments in the public infrastructure and the leveraging of public-private partnerships. Steven Polunsky sees a positive future for passenger rail projects, but warns that evolving and emerging threats must also be addressed. Finally, Armin Cate shares the hurdles associated with guarding international borders and the benefits that innovative solutions can offer. With so many uncertainties for the upcoming year, it is reassuring to know that there are many practitioners forecasting, planning, and readying their communities for whatever is yet to come.

Catherine L. Feinman joined Team DomPrep in January 2010. As the editor-in-chief, she works with subject matter experts, advisors, and other contributors to build and create relevant content. With more than 25 years of experience in publishing, she heads the DomPrep Advisory Committee to facilitate new and unique content for today's emergency preparedness and resilience professionals. She also holds various volunteer positions, including emergency medical technician, firefighter, and member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance).

Publisher's Message

By Martin (Marty) Masiuk

Hang on tight. We are about to go on a wild ride in 2017! Civil unrest, unknown bad actors, cyber vulnerabilities, measuring non-measurables, staff retention, clash of values, evolving diseases, controlling technology, infrastructure failure, and on, and on, and on. Bah humbug! Enough! Time to pause and remember the uplifting story of Charles Dickens' "A Christmas Carol," a story of Ebenezer Scrooge's transformation into a kinder man after being visited by three ghosts. So, to borrow from that outline, here is my publisher's message of DomPrep's past, present, and future yet to come.

DomPrep's Past

DomPrep was founded on the premise that busy people do not have time nor patience to be bothered with content that does not satisfy need or interest. Staying relevant in an era of information overload is always a challenge. In the 2016 readership survey, when asked, "How long have you been a reader of DomesticPreparedness.com, the DPJ Weekly Brief, and the DomPrep Journal," 46.40% have been readers for over four years. That figure is astounding and a good indicator that DomPrep's critical information stays relevant to hungry readers. DomPrep's readership is truly an important demographic, with 67.8% being either in operations or middle/upper management, and 75% are directly involved in the purchasing process. These numbers are a tribute to the many writers and my editor who continue to provide solution-driven content to publish.

DomPrep's Present

To properly serve 10,000+ articles, reports, events, podcasts, and company/government updates, I decided to completely redesign DomesticPreparedness.com. The investment of time and money was well spent. The site is running much more efficiently to better serve the readers. We capture much of this unique content by organizing and hosting by-invitation roundtables, where we uncover tough problems and flush out actionable solutions under the theme, "Creating Value Through Information Exchange."

DomPrep Yet to Come

Preparedness and resilience must and will receive greater priority and increased funding at the local, state, and federal levels. In order for DomPrep to manage the increased logistical challenges, we will partner with Harvard University's National Preparedness Leadership Initiative, the Naval Postgraduate School's Center for Homeland Defense and Security, and the International Association of Emergency Manager's Think Tank program.

As we prepare to celebrate another holiday season and new year, we thank you for supporting DomPrep's ongoing efforts and look forward to working with you in 2017 as we tackle the new issues of the future.

Martin Masiuk is the president and founder of the IMR Group Inc. It was established in 1986. In 1998, Marty created DomesticPreparedness.com (DomPrep), which changed the publishing model by using the internet to reach more disciplines in more jurisdictions than was previously possible. His success with DomPrep gave rise to the Preparedness Leadership Council International, where he serves as the Executive Director.

Authoritarianism & the American Response: 2017 Forecast

By Christopher Milburn

The threats facing the United States in 2017 largely stem from the challenge and response cycle set in motion by the global rise of authoritarianism and violent fascism. Authoritarian leaders frequently promise to restore national pride and return people to their lost golden age: a mythical world in which life was thought to be better for the particular group. Scapegoating quickly follows, and violence is rarely far behind.

Fascism – the harshest brand of authoritarianism usually defined as "ruling by the rod" – takes many ideological forms. Whether religious, political, ethnic, territorial, or usually a combination of these, fascist ideologies seek to carve stark divisions between groups and harshly punish those who are labeled "outsiders." Leaders seeking to mobilize groups to action often utilize violent, divisive rhetoric to inspire in-group pride and provoke action.

Stability & Conflict

The year 2016 has seen a global increase of authoritarianism and fascism. This social phenomenon is, in part, a response to unprecedented globalization that has placed groups into closer contact than ever before. Groups of all types have felt threatened and uncertain, and authoritarianism offers to preserve or restore existing structures for the stability of the group. Globalization and web-based social media have positioned cultures and subcultures of all kinds into types of interactions that were formerly unimaginable.

The year 2017 is likely to see an increase in global authoritarian behavior as groups seek to reverse the effects of globalization and regain honor, resources, and salient identities. Widespread authoritarianism and fascism are very likely to increase group conflict and violence, and homeland security challenges are certain to arise from this dynamic environment of inflamed violent conflict. Two specific current manifestations of authoritarianism pose continued homeland security challenges for the United States in 2017: the continued advance of a violent Islamist global insurgency and the American move toward authoritarianism. These two elements are firmly linked in a challenge and response cycle, and present significant implications for homeland security in a number of ways.

Violent Islamist Insurgency

The Islamic State (IS) remains at the forefront as the current, most prominent patron group of apocalyptic violent Islamism. Originating from a brutal rebranded al-Qaida faction in Iraq, IS arose out of the civil war in Syria, and came into view of the American public in 2014. It quickly identified the United States and its allies as enemies, and has consistently

threatened western nations and religions its leaders consider apostates. IS's brand of fascism identifies enemies of all religions and nationalities – including most forms of Islam – and its brutality toward adversaries is ruthless. IS members are experts at amplifying their symbolic violence through strategic communication, and the group continues to pose a threat as a global insurgency.

Military advances against IS will be important, but conventional warfare is not likely to be sufficient in containing the group. IS is driven by a strong and compelling narrative that remains mostly unchallenged, and the group is skilled in adapting to its circumstances. IS members are particularly effective storytellers who frame their existence squarely within a robust apocalyptic description of world events. In this framework, the group anticipates military challenges and can manage even significant military defeats. Although its media production has dropped somewhat in the past few months, security practitioners should anticipate IS's continued use of a profound strategic communication web to adjust its direction and inspire loyalty from its devotees.

The recent presidential election raises concerns about the growing authoritarianism in the United States and the many uncertainties the country faces in 2017.

The IS threat to the U.S. homeland currently lies in the ability to inspire loosely affiliated individuals within the United States who identify with IS as a religious authority to commit terrorist acts in the name of their ideology. Due in large part to their effective internet-based communication tradecraft, their violence is able to reach deep into the United States in ways unlike any other group so far. This is likely to continue to pose a threat to the United States, even if IS must adapt as its capabilities diminish.

Although the percentage of Muslims who participate in ideologically motivated violence is relatively miniscule, certain violent fascist Islamist ideologies continue to flourish. Violent Islamist leaders have painted a picture of an America that is at war with all Muslims, and U.S. actions are framed as such by some of these ideologues in the Middle East. Efforts to marginalize or exclude Muslims from the United States would only confirm this assertion. As the U.S. president-elect has already made this proposal, the emergence of American authoritarianism is a development that could significantly increase tensions between the United States and the worldwide Muslim community.

American Authoritarianism

The election of Donald Trump to the office of president of the United States could prove to have significant national security implications. Trump campaigned on promises of overhauling a corrupt political system, isolating the United States from its political and trade allies, and restoring America to some former greatness that has been lost. Along the way, he insulted and alienated his opponents to the delight of his staunchest supporters.

President-elect Trump's actions and demeanor have been as erratic and unpredictable as his policy platforms, and he exhibits a pattern of volatile reaction when he is personally offended. If tempered once in office, these patterns could amount to nothing more than hollow campaign rhetoric. But nothing in his history suggests that he will become more stable once he holds the highest political office in the United States. This unpredictability, combined with his blatant ethnic and religious scapegoating, presents a potentially volatile recipe for the U.S. homeland.

Promises of banning Muslims and erecting a border wall are symbolically divisive promises that appeal to a segment of mostly white supporters who feel threatened by social change that they believe is caused by immigrants. His supporters are expecting him to act in office just as he promised he would on the campaign trail. If he attempts to make good on these promises as president, the American identity would be significantly altered both at home and abroad. The response to such action from those who feel threatened by subsequent challenges could be significant – ranging from low-intensity demonstrations that may erupt into violence to more structured violent opposition. Both increased attacks on law enforcement and civil disorder events are perhaps the most likely expressions of this type of response. To date in 2016, the number of law enforcement officers killed in ambush-style attacks is at a 10-year high of 20 deaths. Although there is no comprehensive analysis on the ideological motives driving this trend, an authoritarian social environment is likely to result in more of this type of violent response.

Foreign terrorist groups are particularly responsive to challenges of divisive rhetoric, as well, so Trump's unpredictability may potentially provoke violent responses from Islamists. The IS argues that the United States is at war with all of Islam, and Trump's words about Muslims only serve as evidence that this is true. In addition, IS has also called for attacks on U.S. law enforcement. In this situation, IS seeks to not only launch its own brand of violence within U.S. borders, but it also attempts to exploit divisions already creating conflict between Americans. An unpredictable president is not likely to quell this conflict.


©iStock.com/Violetastock

The possibility for violence from right-wing extremists also exists under a Trump presidency. Trump's rhetoric

has been embraced by white supremacists within the U.S. homeland. If he fails to implement such ideas, or if he backs down from his hardline stances, he faces the potential for a significant backlash from betrayed right-wing nationalists. Violence and unrest in this case could very likely be directed either toward representatives of the U.S. government (out of a sense of betrayal) or at minorities (out of anger or fear).

Conversely, actual implementation of policies such as a religious ban could legitimize white supremacist ideals in the eyes of the violent right wing. A president suggesting that religious practitioners from the Middle East should be registered or banned from entering the United States could be taken as implicit inspiration to dehumanize and harm that group within the United States. The days after Trump's election have seen an increase in racially motivated violence, and more of this type of violence is a distinct likelihood. In either case, Trump's themes of scapegoating and isolationism have placed the United States in a precarious security position in which increased violence of some kind is likely.

Ultimately, Trump's election to office represents both the United States' willing participation in the global splintering of authoritarianism as well as a response – based in fear and anger – to threats perceived by many Americans. Rhetoric that legitimizes white American nationalism plays into multiple narratives including those of white supremacists, disenfranchised domestic minorities, certain foreign sovereign nations, and violent apocalyptic Islamists. This is likely to significantly inflame tensions between many groups both within the homeland and around the globe.

What to Expect

Security practitioners should anticipate a social climate of heightened tensions and an amplified violent challenge and response cycle in 2017. Social structures continue to unravel, mistrust in social and political establishments continues to climb, and the globe is bristling with reactionary authoritarians at the helms of their various sovereign nations. The year 2017 will most likely see the continued – if not even a punctuated – increase in domestic civil unrest and terrorist acts within the United States. Effective homeland security measures will depend on accurate analysis of global events, careful monitoring of extremist rhetoric – particularly from white nationalists, Islamist extremists, and disillusioned domestic groups – and a clear understanding of the effects of U.S. actions both at home and abroad.

Disclaimer: This forecast is based on research conducted on symbolic violence and the nature of mass movements, as well as an assessment of current social conditions as viewed in the analytical framework of Social Identity Theory.

Christopher Milburn is a fire captain in Long Beach, California, where he has served as a public information officer and terrorism liaison officer. He is a graduate of the U.S. Naval Postgraduate School's Center for Homeland Defense and Security with an M.A. in Security Studies, and has a B.A. in Communications. His terrorism research has focused on strategic communication, information operations, social identity, culture and religion, and symbolic warfare.

Bombing an Ideology: No One-Size-Fits-All Approach

By Richard Schoeberl

Stretching from Belgium to France, the United States to Iraq, the world has been blemished with terror attacks ranging from active shooter scenarios at entertainment venues, to plowing vehicles into crowded streets. Over the past decade, the United States has joined the global community of those exposed to the consequences and carnage associated with acts of terrorism.

Although many in the world view terrorism as a form of violence that only imposes psychological and physical impacts on the communities it touches, it is equally important to keep in mind the financial impact of terrorism – exceeding $180 billion globally over the past two years. The costs associated with terrorism are equivalent to the 2011 Fukushima nuclear disaster cleanup in Japan, the same cost associated with the rebuild of Syria, and comparable to the annual value of cargo that passes through the Port of Long Beach – one of the world's busiest seaports. In fact, to put it into perspective – the economic costs associated with terrorism exceed the GDPs of most countries, including: New Zealand, Uzbekistan, Ecuador, Luxemburg, and Jordon. Aside from the psychological impact, terrorism comes at a cost – both physical and fiscal.

Polls & Statistics

Trends associated with global acts of terrorism tend to present complex problems for experts analyzing the impact of imminent threats – and at no time in history has there been this much uncertainty. For analysts and U.S. citizens alike, fear and an increased level of uncertainty remain. According to a Gallup Poll taken shortly after the events of 9/11, nearly 60 percent of U.S. citizens felt vulnerable to terrorism and expressed a sense of fear that the United States would likely see another terror attack on domestic soil within weeks. That fear leveled off over the years, but the Gallup Poll later indicated at the end of 2015 that some 50 percent of U.S. citizens still feared that a terrorist attack could happen on domestic soil. Following the attacks in Brussels, Belgium, in March 2016, the same 50 percent of U.S. citizens polled feared a terror attack in the United States was imminent.

Regardless the level of fear, most concerning is the question, "Will an attack on the United States actually happen?" At no time in recent history, since the attacks of 9/11, has the United States faced a greater risk from Islamic extremists as it does right now – chiefly from those "radicalized" within the United States. The Islamic State's (IS) paradigm shift – from preaching for people to come abroad and wage Jihad, to the most recent message of waging Jihad in the home country – has led to the influx of domestic attacks. Over the past two years, there have been over 160 IS-linked terror plots against Western targets.

The House Homeland Security Committee released the Committee's December 2016 Terror Threat Snapshot, which forecasts increased threats for both the United States and Europe. During this past year, the IS carried out more than 60 attacks within the United States and Europe, attributing to over 700 critically injured and over 200 confirmed deaths. Furthermore, according to the Committee's report, law enforcement has arrested more than 100 people in the United States in IS-linked investigations since 2014. In 2016 alone, 35 people were arrested in 18 separate states for IS-linked investigations.

Feeding Fear & Uncertainty

Fear in the United States emerges from people who previously were not reachable before, but can now be easily reached through social media and "slick" propaganda. A recent magazine, *Rumiyah* (published by the IS), calls on would-be Jihadists to embrace sharp objects – or available weapons – to carry out lone-wolf operations wherever they are, suggesting they do not need to travel abroad to assist in the Jihad. The magazine, which is shared online in PDF form, suggests a "campaign of knife attacks." The IS has additionally released a propaganda video instructing followers that they do not need sophisticated weaponry to launch an attack in support of the cause, but can utilize what is already available. In response to the recent report released by the Homeland Security Committee, Committee Chairman Michael McCaul (R-TX) stated:

> *The attack last week at Ohio State University is further proof that our homeland remains in the crosshairs of Islamist terrorists. Groups like ISIS are radicalizing new operatives from within our borders, and just this week their new spokesman called for more inspired attacks by supporters "all over the world." Make no mistake: we face a deadlier threat than ever before not only because our enemies have gotten savvier, but because we took the pressure off them. For eight years, the Obama Administration reluctantly played global whack-a-mole with terrorists rather than leaning into the fight with decisive leadership. Because of this, the Trump Administration will inherit a generational struggle that has only gotten longer. But rest assured, we will work closely with them to turn the table on these fanatics.*

With no strategy in place to combat IS for the past several years, coupled with IS's growth in popularity, there is no uncertainty that the organization will continue to remain a threat in 2017. Currently, some 34 Islamic extremist groups have pledged allegiance to the IS and the organization continues to grow in strength with franchises and auxiliary groups established in Yemen, Tunisia, Syria, Sudan, Russia, Philippines, Pakistan, Palestine, Nigeria, Lebanon, Libya, Jordon, Iraq, Indonesia, India, Egypt, Brazil, Bangladesh, Algeria, and Afghanistan. The West will continue to remain a vulnerable target for Islamic extremist groups in 2017 because of several factors:

- *Recidivism* – In 2016, the current administration relocated 48 prisoners from Guantanamo Bay (GTMO) Detention Center in 2016. The director of national intelligence estimated that at least 30 percent of GTMO detainees are alleged to have resorted back to terrorist activities. There are currently only 59 prisoners remaining at GTMO.
- *Rehabilitation, the United States makes no attempt* – The director of intelligence's most recent assessment of recidivism revealed that one-third returned to terrorism. Several terrorist rehabilitative programs worldwide have been established with the hopes of reforming radical Islamic extremists. Several years following the attacks of 9/11, realizing the increasing popularity in Islamic extremism, several countries such as Iraq, Singapore, Saudi Arabia, and Indonesia all developed terrorist rehabilitation programs – or de-radicalization programs. These programs are deliberately designed to align behavior and thinking to a more nonradical and nonviolent ideal. They are comprised of several approaches directed at changing the extremist's interpretation of Islam, distancing that person from the extremist group he or she was a part of, and most importantly reintegrating that person back into mainstream society. The country renowned as having the most complete and successful terrorism risk-reduction strategies is Saudi Arabia. The United States does not have one in place, nor did the GTMO Detention Center.

With physical, psychological, and financial implications, terrorism increases fear and uncertainty for Western nations in the upcoming year.

- *Refugee Flow* – The United States cannot vet the number of refugees seeking entry into the country. In 2016, the Obama administration has immigrated close to 13,000 Syrian refugees into the United States. Intelligence officials have repetitively indicated that the United States lacks the reliable means to appropriately screen and vet the possible Syrian refugees seeking entry. The National Counterterrorism Center (NCTC) acknowledged that, individuals with ties to terrorist groups in Syria attempting to gain entry to the United States through the U.S. refugee program.

- *Porous Borders* – The question is, "How can we effectively secure 2,000 miles of the Southwest border?" In an area that stretches from California to Texas – encompassing more than 2,000 miles – the border between the United States and Mexico remains porous and unsecure. IS militants have raised awareness among its followers that entry into the United States through the Southwest border is a viable option.
- *Homegrown extremism* – As the IS looks for means to enter the United States through traditional travel methods, southwest border smuggling routes, or refugee status, there is still concern with the marketing methods and propaganda that radicalize over the internet and recently prompted the attacks in Chattanooga (Tennessee), San Bernardino (California), Orlando (Florida), and Ohio State University. Orlando gunman, Omar Mateen, watched IS propaganda online and pledged his allegiance to IS leader Abu Bakr al-Baghdadi. There is no doubt that social media has revolutionized terrorism through its ability to radicalize those who were previously unreachable around the globe.

Contributing Factors for Radicalization

Terrorism and radicalization are no longer a law enforcement issue, as police can only do so much to protect an exposed society from violent extremism. Law enforcement can no longer be expected to work alone in addressing this threat. Officers simply cannot watch all people, all of the time – only some of the people, some of the time. As a society moving into 2017, people must now recognize and report signs of radicalization. Although religion plays a marginal role in the radicalization process, most people are driven by political or social change, grievances, personal dissatisfactions, and sense of adventure – which is clearly what Islamic extremists exploit.

These people adopt extreme social, religious, and political viewpoints, thus rejecting contemporary ideas. Other contributing factors involved in the radicalization process include: life-altering events, social networks, poverty, unemployment, and charismatic clerics – such as Anwar al-Awlaki. There really is no "simple" explanation behind radicalization, as different people follow different paths to get there. Regardless *how* someone is radicalized, it will be an increased threat to recognize going forward. The United States under new leadership will need to embrace a multitude of strategies to combat the ever-looming threats facing U.S. communities. The one-size fits all approach of "bombing an ideology" has not worked thus far.

Richard Schoeberl, a Ph.D. candidate in criminology and terrorism, has over 20 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 in 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.

Unmanned Aircraft Systems for Emergency Management

By Darren E. Price

Responding to disasters is a critical function for first responders and the emergency management community. Rotary and fixed-winged aircraft have traditionally performed disaster response missions, such as overhead damage assessments, reconnaissance, and missing person searches. However, with the advancement of unmanned aircraft systems, there is an opportunity to perform conventional aerial missions in a safer, expeditious, and cost-effective manner.

Emergency managers are tasked with protecting the communities they serve – through planning, training, exercises, and technology. However, one technology has yet to be fully leveraged: unmanned aircraft systems (UAS).

Advantages & Uses

Rachel Finn and David Wright of Trilateral Research & Consulting LLP in London, UK, published a 2014 study stating that, "UASs have a 'niche' in performing the three Ds: dull, dirty, and dangerous work." Additionally, in 2003, Aviva Brecher at the U.S. Department of Transportation's Volpe Center offered that UASs can be deployed on demand, have flexibility in tasking, have plug and play capabilities for their payloads, can support high-resolution cameras, and can cover remote areas. These are but a few examples of the advantages and potential uses for UASs.

One advantage offered by UASs in comparison to rotary and fixed-winged aircraft is their ability to obtain unique observation angles that are not practical or otherwise possible via conventional means. UASs can be, and have been, used for a variety of missions, including agricultural inspections, assessing critical infrastructure, determining building and structural integrity, and conducting preliminary damage assessments. Recent real-world examples exhibiting the use of UASs for emergency management-related missions include UAS use to aid in:

- Recovery efforts by the U.S. Army Corps of Engineers during the October 2015 flooding in South Carolina;
- Relief efforts in the aftermath of magnitude 7.8 earthquake in Nepal in April 2015;
- Missing person searches; and
- Damage assessments at the Fukushima Daiichi nuclear power plant from the March 2011 earthquake and resultant tsunami that struck northern Japan.

Additionally, collapsed buildings pose an especially hazardous situation for emergency responders due to the instability of the structures. The use of UASs provides an alternative to sending emergency responders into an unstable building environment to determine

its stability, with the added benefit of being able to provide real-time audio/video and environmental sampling. Not only does there appear to be an emerging interest in using small UASs for structural assessments, a 2014 article published in the *Journal of Field Robotics* noted that experiments have indicated that small UASs have been able to enter the hot zone of contaminated areas and begin transmitting usable data within 16 minutes. This is a significant finding as this timeframe is considerably faster than what traditional hazardous materials or radiological monitoring teams can accomplish.

In addition to traditional emergency management missions, the use of UASs represents a force multiplier for fire departments that deploy an air reconnaissance chief (ARC) during fire response operations. As an example, the current policy of the Fire Department City of New York (FDNY) is to deploy a battalion chief, operating as the ARC, for high-rise business and residential fires, as well as for building collapses. The activation of an ARC can also occur for multiple alarm fires, weapons of mass destruction incidents, special events, and incidents spanning large geographic areas that are otherwise inaccessible. The role of the ARC is to provide an overhead scene assessment (e.g., imminent hazards, structural integrity, location[s] of building occupants) to the incident commander (IC) on the ground. This assessment is critically important to the IC, as it will assist with guiding the priorities, objectives, strategies, and tactics comprising the incident action plan. The deployment of a UAS would decrease the time necessary to obtain an on-scene assessment or situational awareness, thereby expediting the sharing of incident information (e.g., live video feed, telemetry) with the incident command post and emergency operation center(s).

Barriers to Implementation

There are numerous barriers that complicate the use of UASs for disaster response, including public perception (i.e., privacy concerns), current Federal Aviation Administration (FAA) rules and regulations, and a general lack of organizational policy structure. Although none of these areas is insurmountable, they nonetheless represent challenges for agencies considering the use of UASs within the United States. Among various barriers that exist, two of the more challenging ones are privacy concerns and the current FAA restrictions on the use of UASs by government agencies.

Privacy concerns have been raised that the domestic use of UASs may infringe upon the right to privacy afforded under the Fourth Amendment to the U.S. Constitution. Recognizing public concerns about the use of UASs to conduct domestic spy missions, the U.S. Department of Homeland Security has proactively assigned the Office for Civil Rights and Civil Liberties and the Privacy Office to lead a working group ensuring the domestic use of UASs does not violate individual rights

to privacy. The Obama Administration has taken this a step further through the issuance of a 2015 presidential memorandum that recognizes the need to promote innovation and "economic competitiveness" regarding the domestic use of UASs, while at the same time providing protections for privacy, civil rights, and civil liberties.

An additional barrier complicating the use of UASs for disaster response missions in the United States is the FAA restrictions on the use of UASs by government agencies. There are processes for emergency requests, but the typical turnaround time to obtain a non-emergency Certificate of Waiver or Authorization (COA) for government agency UAS use is approximately 60 days. Even with a one-time emergency waiver, the timeframe required to obtain a COA is mission prohibitive for real-time response to disasters and presents a significant barrier to agencies that may be interested in using UASs for immediate disaster response missions. Furthermore, the interpretation espoused by the FAA – that a UAS operated by a civilian hobbyist is not an aircraft, but one operated by a government agency is – represents a clear contradiction in logic that must be addressed if UASs are going to be used to their full potential.

Emergency managers have the opportunity to leverage unmanned aircraft system technology to further public safety efforts.

Decision Guide for Emergency Managers

With an opportunity to be on the leading edge of the UAS revolution, it is an exciting time to be in emergency management. The field of emergency management should move forward with the establishment of UAS programs for disaster response by embracing UAS technology and the many benefits it offers for mitigation, preparedness, response, and recovery mission operations. Although the necessity to regulate the use of UASs in the national airspace system is recognized, such regulation cannot stymie the implementation of UAS programs for government agencies, especially for programs focused on public safety functions such as disaster response.

The author's Naval Postgraduate School master's thesis, entitled "Unmanned Aircraft Systems for Emergency Management: A Guide for Policy Makers and Practitioners," contains a guide in the appendix that serves as a tool to help policymakers and practitioners determine the need and feasibility of implementing UAS programs in their agencies. It also serves as a practical job aid that leads policy makers and practitioners through various decision points to consider when assessing the need and feasibility of a UAS program.

Elements of this article were previously published in the June 2016, International Association of Emergency Managers (IAEM) Bulletin, the official monthly newsletter of the IAEM.

Darren E. Price, MA, is an emergency manager and regional supervisor with over 30 years of public service, including 15+ years in emergency management. He is a graduate of the Naval Postgraduate School's Center for Homeland Defense and Security Master's Program, where his thesis, "Unmanned Aircraft Systems for Emergency Management: A Guide for Policy Makers and Practitioners," was an outstanding thesis award nominee.

Making the Grid Great Again

By J. Michael Barrett

As the dust from the recent election settles, one of the first orders of business for the incoming Trump administration is a massive public infrastructure investment plan. Although the economic benefits associated with improved infrastructure are popular with many citizens and both sides of the political aisle, the real-world practicalities of ensuring positive economic return from such investments are nonetheless daunting.

Specifically, three major considerations must be addressed: (a) where to focus the investment; (b) how to finance the projects; and (c) how to produce viable long-term benefits. It stands to reason that infrastructure revitalization efforts should be aimed at projects that improve conditions for large portions of the general public as well as address the needs of private sector businesses in order to ensure that the United States remains economically competitive. Although the visible disrepair of roads, bridges, and airports gets much of the public's attention, those making decisions would do well to consider an active role in managing the unseen but increasingly crucial issue of reinvigorating – or, indeed, reinventing – the nation's power grid.

Securing the Power Grid: Past, Present & Future

Given the enduring nature of power grid infrastructure investments, the full opportunities and benefits of a secure, resilient, and modern power grid hold much promise for years to come. In fact, with many custom-designed but decades-old components of the current national power grid system having reached their maximum useful life at the same time as local power generation, enhanced grid cybersecurity, and the coming wave of internet-enabled "smart grid" technologies are all converging, the timing to focus on this industry could hardly be better. It would be a great accomplishment indeed to focus on ensuring that the United States develops the required modern electrical power backbone to meet the needs of the next 100 years.

Consider that the current U.S. model of a mostly centralized and highly regulated electrical power industry relies on industrial-age ideas about leveraging size to provide affordable power across the country, and yet today the world is much more mobile, fluid, and flexible. In fact, the nation is already in the early stages of a two-decades-long modernization effort that will spend a projected $2 trillion to replace many aging pieces of the current electrical power grid infrastructure – a massive investment that offers a rare opportunity to re-think how the whole system of power generation, delivery, and usage operates. Further, given that it is always more cost-effective to build in new technologies and features than to retrofit them later, a clear-eyed strategic effort to make the most of these investment dollars would ensure

both improved operations as well as systemic improvements in resilience, survivability, and integration of secure cyber solutions. At the same time, developing the intellectual property by designing the new architecture and solutions for tomorrow's grid at home could ensure the U.S. remains a world leader in meeting growing global energy demand for decades to come.

Similarly, there is rising concern over the negative externalities of the current power grid, including quality and reliability, environmental impacts, resilience against prolonged system-wide disruptions, and the energy wasted by outdated generation and transmission equipment. As a result, the economics that underpin the United States' current and future means for generating, transmitting, and delivering reliable, stable, and affordable electrical power are undergoing a period of significant change. The time is right to develop a new, more modern architecture that includes a combination of microgrids, localized renewable energy sources, and end-user access to even more stable and secure energy.

Tailored Public-Private Partnerships

Having identified the grid as a worthy area of focus, there is also the challenge of how best to finance all the myriad investments required to achieve significant change. The answer here lies with the often discussed but also often poorly understood concept of tailored public-private partnerships. Although the term may seem complex, all it really means is that by combining forces for a specific project it is possible to share each parties' inherent assets in the way that best offsets their shared liabilities. For example, if the federal or state government can reduce the investment risk of the project by providing seed capital, issuing tax-exempt bonds, and/or signing a letter of intent to purchase energy for a guaranteed period of time, the private sector can then provide investment capital at more favorable rates because total project risk is reduced.

Public-private partnerships allow a broad mix of partners to share overall benefits, including:

- ***Improved usage of available public land;***
- ***Tax-free bonds for investors;***
- ***Tax credits for environmentally beneficial projects; and***
- ***Government and industry's recognized ability to meet community needs.***

In this way, all the involved parties share the up-front construction costs, promote open access to usable land, and lock-in the commitment of long-term users. Similarly, if a military base, civilian manufacturing facility, and local municipal critical infrastructure are all sharing a purpose-built microgrid, they could, for example, take best advantage of excess land owned by the base while: (a) sharing tax credits that offset investment costs borne by the private sector; and (b) ensuring that the energy produced is optimized to meet local municipal needs and sustain a local effort to develop new industrial capacity.

Ultimately, investing in the overall industrial sector of energy generation and distribution by funding domestic infrastructure improvements represents an important mix of new technologies that can significantly improve the operation and cost-benefit analysis of ensuring the robust, resilient delivery of "always-on" clean energy. Just as importantly, owning the designs, patents, and know-how about the underlying technologies of the smart grid also will allow for sustained economic advantages. Therefore, as the incoming administration considers where and how to make investments that best prepare this nation for the future, a large-scale public-private partnership supporting the innovation and creativity associated with burgeoning energy technologies and the "smart grid" would be a smart place to start.

J. Michael Barrett is director of the Center for Homeland Security & Resilience, an adjunct scholar with the Lexington Institute, and a former director of strategy for the White House Homeland Security Council. Serving as a Naval Intelligence Officer in the aftermath of the terrorist attacks of 11 September 2001, he worked on a variety of programs aimed at defeating terrorists overseas before transitioning to homeland security and developing core strategies and policies enabling a risk-based posture for federal, state, and local efforts. His recent work includes authoring Lexington's "Future of the Power Grid" series. A former Fulbright Scholar, author or co-author of two books, many White House, Department of Defense, and Department of Homeland Security strategies, and dozens of terrorism and homeland security articles, he also has been a frequent national security guest on television programs including ABC, Bloomberg, CNN, CNBC, Fox News, and Nightline. He can be reached at mbarrett@security-resilience.org

The Year of the Railway Station

By Steven Polunsky

The year 2017 should be a great year for mobility and infrastructure in the United States. All signs are pointing to a robust economy, and policymakers are looking favorably on transportation projects – road, rail, air, public, private, and in between. In particular, the upcoming year will see a number of passenger rail projects moving forward.

Significant and highly visible high-speed intercity passenger train projects are in the planning stages in Florida, California, Texas, and states in the Northeast. There is even a proposed magnetic levitation train in the Northeast Corridor. These projects are not going to magically appear in a protective bubble, however. Threats are real and documented, and 2017 may be the year when international terrorism retools for U.S. passenger rail.

Warnings With Cyber & Physical Attacks

Vulnerabilities abound within the passenger rail sphere. Cybersecurity events such as the November 2016 hacking of the San Francisco Municipal Light Rail System that forced Muni to suspend charging for rides, and transitional periods like the implementation by commuter railroads of positive train control suggest areas for attention by security interests, as do systems increasingly dependent on electric grids and electronic backends like passenger ticketing. Trains in transit have been platforms for onboard terrorist efforts like the August 2015 foiled armed attack on the French TGV as well as attempts to attack the right of way and blow up the rails (TGV in 1995), some successful (Muniguda, Munikhol, and other incidents in India in 2015).

> ***In 2017, it is time for the railway station to garner the same level of focus on security as other routes of transportation have over the years.***

Perhaps the best case to be made for 2017 is for a focus security efforts at stations, where there will be large masses of people. For example, the Texas Central project calls for eight-car trains carrying 200 people with rush-hour departures every 30 minutes. Terrorists could exploit such station vulnerabilities – for example, a coordinated knife attack inside the Kunming station (China) in 2014 killed 29 civilians and injured more than 140. Twenty people died in the bomb attack on the Maelbeek Metro station in central Brussels in March 2016. A 2011 Inspector General's report criticized how Amtrak and the Department of Homeland Security were spending security money, concluding, "The traveling public remains at risk for a potential terrorist attack at Amtrak's high-risk stations."

Decisions & Innovative Thinking Going Forward

Yet, there is little indication that high-speed train stations – "Palaces of Transport," according to the U.S. High Speed Rail Association, and "iconic structures" per the Texas Central Railroad – are benefitting from innovative thinking when it comes to security. California High-Speed Rail's Request for Qualifications for the High-Speed Rail Systemwide Vision Plan for Stations of 2015 talks about world-class sustainable public places, but does not mention safety or security. Texas Central held a design competition in 2016 among university architecture, engineering, and transportation programs, with judging based on programming, urban connectivity, use of local materials, environmental sustainability, and customer focus. Security was nowhere in the mix.

There is a continuing debate about the relative merits of airline-style security measures (landside/airside separation, personal and baggage screening, metal detectors, and radiation devices) as opposed to current practices for surface transportation like rail and bus. Even so, there are generally accepted approaches, some as an outgrowth of incidents like the Tokyo (Japan) sarin gas attack of 1995 – adding surveillance cameras, revising training and response protocols, removing trash cans where bombs can be hidden, controlling access to secured areas, providing two-way communication through public address systems and call boxes, intrusion detectors, and so forth. Advocates for both sides argue the relative merits of multilayer security, level of separation from vehicle side and groundside, and level of identification with boarding passes, as well as whether security queues and baggage checks are even realistic for train operations.

It is time to wrap up these conversations and move forward with innovation in station design. Hopefully, 2017 will be remembered as the year that new, secure stations were planned from the ground up.

Steven Polunsky (Twitter: @StevenPolunsky) is a research scientist with the Texas A&M Transportation Institute's Policy Research Center. He previously directed legislative committees overseeing transportation, homeland security, and regulatory policy where he led an award-winning technology initiative that saved thousands of taxpayer dollars. Prior service includes director of research and planning for the Texas High-Speed Rail Authority and legislative policy analyst for the Texas Department of Transportation. He has an MPA from the LBJ School of Public Affairs as a Robert Strauss Fellow and an MA in Security Studies with Distinction from the Naval Postgraduate School.

WELCOME TO THE FAMILY, LITTLE GUY.

The world's most trusted range of radiation detectors just got bigger — and tougher. Introducing the fully IP67-rated FLIR identiFINDER® R100 personal radiation detector. Experience the power of tough.

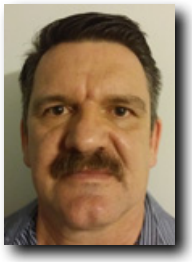
www.flir.com/identifinderR100

FLIR® | The World's Sixth Sense®

Noncriminal Alien Self-Identification Program

By Armin Cate

The removal of criminal illegal aliens is a top priority for President-Elect Donald Trump. However, identifying, locating, processing, and deporting 3 million criminal aliens among the 20 million illegal aliens in the United States would completely overwhelm the removal process currently in place. One proposed program may help speed the processing of criminal aliens and prevent the deportation system from imploding.



The Noncriminal Alien Self-Identification Program (NASIP) is a proposal that would allow noncriminal aliens to self-identify, thereby significantly reducing the number of illegal aliens that government investigators would have to search for in order to identify, locate, and process criminal aliens. To eliminate fraud, all applicants would be subject to a background check by a private contractor, followed by an independent verification by Immigration and Customs Enforcement (ICE). It would also allow noncriminal aliens to choose self-deportation and, in exchange, allow them to apply for visas to the United States without penalty upon returning to their countries of origin.

A key component of NASIP would be to create a new non-immigrant visa class that allows noncriminal illegal aliens to obtain temporary legal status in exchange for self-identification. Essentially, this new non-immigrant status would be similar to the current Temporary Protected Status (TPS), which could be used in place of creating a new visa category. Providing noncriminal aliens with non-immigrant visas is preferable to the current process of ICE issuing only a Notice to Appear (NTA) because it provides noncriminal aliens with temporary legal status. This would allow illegal aliens to come out of the "shadows" to pay taxes, obtain drivers licenses and car insurance, and possibly even travel overseas. Another important benefit would be that their appearance before immigration judges would be held in abeyance until all criminal aliens and the other noncriminal aliens that did not self-report had their cases heard and adjudicated.

Once aliens have self-identified, ICE would provide that information to private companies contracted to conduct background checks using state-licensed private investigators. After checks are complete, the federal contractors would create case files and provide them to ICE. Any aliens that self-reported and were found to have criminal records would be immediately detained and have their files forwarded to immigration judges. ICE in turn would conduct independent verification checks utilizing national agency and anti-terrorism databases (these checks determine if there is an open investigation) on the applicants and then forward the files to U.S. Citizenship and Immigration Services (USCIS). Once an illegal alien has been

verified as noncriminal, USCIS would provide them with the new temporary non-immigrant visa. ICE would still issue NTAs to set up initial appearances before immigration judges, but these NTAs would be placed in the cue in such a way that all criminal aliens and noncriminal aliens that chose not to self-identify would always be given priority.

Currently, the removal process can take a few months to a few years depending on the ongoing case log and the length of the appeals process. Once the push to deport 3 million criminal aliens begins in earnest, and a process such as NASIP is put in place, the main chokepoint would then be the number of immigration judges available to hear cases. As the system becomes backlogged with millions of criminal cases and millions of noncriminal cases during ICE deportation operations, the removal process for self-identifying noncriminal aliens could easily take as long as five or more years. Often, during operations to locate and capture criminal aliens, more noncriminal aliens than criminal aliens are apprehended by ICE agents simply because they live at the same address or work at the same location.

Deporting millions of illegal immigrants is a monumental task. However, a new innovative idea could help overcome some of the impending hurdles.

Under these circumstances, another important benefit provided by NASIP is that verified noncriminal aliens who self-identified and are caught in the net of ICE operations, would not be detained and their NTA would not be forwarded to an immigration judge for immediate deportation. Instead they would be released as long as they had not committed felonies or are not suspected of having committed any criminal acts. As previously stated, their cases would not come before immigration judges until all other cases are heard. This could be one of the main factors that would influence applicants to favor this program. Another key factor is that, once they are deported, their participation in NASIP will provide them with a way to return to the United States legally much faster by allowing them to apply for visas in their country of origin without a black mark on their record.

The temporary legal status as the result of this new non-immigrant visa would not only allow people to apply for visas after deportation, more importantly it would allow them to come out of the shadows. Not only would it incentivize them by being able to live without the fear of immediate deportation while their cases await their turns in immigration court, but it would also allow verified noncriminal aliens to apply for drivers licenses, obtain temporary employment authorization, pay taxes, and travel back to their home countries. These are all benefits that would make this program attractive to potential applicants and, in return, would solve a number of problems that noncriminal aliens create by living in the shadows – for example, driving without a license and insurance, not reporting wages earned, or not paying taxes for the use of local schools, roads, and medical facilities.

Benefits for Immigrants & for the Country

In addition to benefits for noncriminal aliens who apply for NASIP, the U.S. government would benefit from savings in the millions of dollars as well as a reduction in the backlog of cases in immigration court. The reduction in the backlog occurs when noncriminal aliens choose to self-deport, with the option to apply for return visas without penalty. The monetary savings comes into play by utilizing state-licensed private investigators (there are approximately 41,500 in the United States) instead of federal agents or contracted professional background investigators to verify the information submitted by noncriminal aliens. Utilizing state-licensed private investigators that work for federal contractors keeps the federal government from having to hire hundreds if not thousands of new federal agents for what is essentially a "temporary situation" or pay a much higher hourly rate for contracted professional background investigators. This alone could save the United States millions of dollars. It would also save time by freeing time for federal investigators to concentrate on locating the criminal aliens.

NASIP would save the federal government a significant amount of time and money by:

- Having private investigators, who are paid at lower hourly rates than federal investigators, conduct "pre-certification" investigations;
- Freeing time for law enforcement officers to locate and remove criminal aliens; and
- Saving law enforcement agencies time by reducing the pool of illegal aliens that law enforcement would have to review in order to locate criminal aliens.

Below are the suggested benefits to the noncriminal aliens who register for this voluntary self-identification program:

- After they are vetted and limited background checks show that their answers are truthful, they will be "pre-certified" and allowed to apply for newly created non-immigration visas after their records are reviewed and approved by immigration judges.
- After they have completed the self-identification process, they are "pre-certified," their initial case files are reviewed and approved by immigration judges, then they are able to apply for the new non-immigrant visa category.
- They will be allowed to remain in the United States under legal status until immigration judges hear their cases.
- Their cases will go to the bottom of the immigration case lists and always remain behind the illegal aliens who did not self-identify.
- Pre-certified" illegal aliens who desire the fast track to self-deportation would have no consequences when applying for future visas to re-enter the United States.
- If illegal aliens or their immediate family members are randomly detained as illegal immigrants, they would be released on their own recognizance

awaiting their immigration hearings as long as they are not facing criminal charges and have not committed new felonies.

- They could receive legal assistance from immigration attorneys contracted by the U.S. government at no cost.
- They could receive an Employment Authorization Document (EAD) to be renewed annually.
- They would continue to be allowed to use the public and private school system.
- They could obtain identification documents that would allow them to acquire state drivers licenses.
- They could have access to the public health system.
- They could obtain social security or tax identification numbers for the purpose of paying income taxes.
- They could travel internationally.

To facilitate NASIP would require forming a working group to include representatives from federal, state, and local law enforcement agencies responsible for the enforcement of laws and regulations that apply to illegal aliens. Nongovernmental organizations that represent immigration issues as well as churches and academia could also be invited to participate. This group would oversee the creation of NASIP, which is essentially a database for noncriminal immigrants who want to self-identify because they have committed no other crimes. These noncriminal aliens would like to identify themselves and their immediate family members to the U.S. government in order to qualify for what would be a newly created non-immigrant visa category that would provide them with a temporary legal status. This would be a limited and conditional status allowing them to receive benefits until immigration judges have adjudicated their cases.

Immigration Reform, Not Amnesty

In conclusion, NASIP is not an amnesty program that welcomes more people into the United States and should not cause a surge in illegal immigration. It is a temporary non-immigrant legal status, similar to the current Temporary Protective Status (TPS) but more effective. It does not guarantee amnesty to people who voluntarily self-identify as illegal aliens and there is no guarantee that noncriminal aliens who participate in NASIP will not be deported at the end of the process. However, their cases would be positioned in the immigration court system in such a way that cases for nonparticipating illegal aliens would be adjudicated first.

Although this program would put illegal aliens who self-identify into the immigration removal process, it would also provide them with temporary legal status to remain in the country until their cases are heard. Once they are "pre-certified" for not having criminal backgrounds, not suspected of having committed felonies, not facing criminal charges, and/or not having committed felonies in the past, their cases would remain at the back of the cue until all illegal aliens who have criminal records or who have not self-identified have had hearings. In addition, a yearly review process could be implemented to ensure participants have not committed any new criminal acts while their cases await hearings before immigration judges.

That removal process for applicants for NASIP could take years once the U.S. government begins the process of removing the three million criminal aliens living in the United States. During that time, they would be living out of the shadows. They would be fully identified and would no longer be a problem to motorists by driving without licenses or insurance. Among the benefits to the United States could be millions in savings in money and manpower as well as the speedy location and removal of dangerous criminal aliens. In return, noncriminal aliens would receive a number of benefits including release from detention and immediate deportation should they be caught in a federal operation targeting criminal aliens. Although this is happening with current policy, the current system would collapse with a significant increase in NTAs being issued. Another benefit to consider could be allowing noncriminal aliens that waited more than five years for their cases to be completed to apply for permanent resident cards. Once they have had their initial hearings with immigration judges, they would apply for permanent or some type of temporary status.

NASIP was designed based on years of experience developing successful local, regional, and national public-private partnerships during 28 years of service with ICE and the U.S. Coast Guard. In cases like this, where the government system is overwhelmed both from a manpower and social standpoint, forming a partnership with private agencies and nongovernmental organizations can be the key to success. These problems can be quickly diffused by sharing responsibilities with other stakeholders and by allowing private partners to take the lead, especially with regard to dealing with the media in highly controversial situations.

Armin Cate is a 34-year veteran of the Department of Homeland Security (DHS), retiring as a special agent with Homeland Security Investigations Immigration and Customs Enforcement and as a commander with the Coast Guard Reserve. Prominent among his achievements was the detection and apprehension of Sayed Malike, a terrorist at the Port of Miami in March 2003. Since retiring from DHS, he has served as a consultant on border security for the transition team for Mexican president Pena-Nieto and has been a key member of design teams developing complex security solutions for airports, seaports, and intermodal transportation – including the modernization of the Air Defense system for Mexico and designing a secure rail corridor across the U.S./Mexican border. Trained by the Secret Service as a member of the JUMP team for presidential candidate George W. Bush, he has led executive protection teams for a Fortune 100 CEOs traveling to Colombia, Mexico, and Brazil. He has worked as a consultant for sales and marketing for several manufacturers of cutting-edge, high-tech security products including Thermo-Scientific. He also provided protective services at the 2014 Sochi Winter Olympic games, along with five former members of U.S. Navy DEVGRU, Seal Team Six.

Preparing for a New Pandemic With an Old Plan

By Robert C. Hutchinson

The measurable level of national planning and preparedness for a serious pandemic threat or biological attack continues to be a subject of great discussion, debate, and concern in the United States and around the world. This level of readiness continues to be a challenge as identified in regular studies, reports, and articles.

A review of the valuable daily and weekly collection of articles and reports from UPMC Center for Health Security, Global Biodefense, ProMED, and other valuable information sharing organizations provides additional evidence of the emerging and re-emerging global health threats and many areas for improvement. As these public health threats expand in an exceptionally globalized world of rapid trade and travel, the level of preparedness becomes even more critical and essential. Unfortunately, a review of the public health headlines and findings each day often does not provide a great deal of comfort.

Beyond negative reports, and at times overly dramatized articles, there continues to be legitimate reasons for concern for lessons do not appear to be learned and recommendations are often shelved with the completion of a strategy or report. Even though it appears that the Zika virus has replaced the Ebola virus as the public health threat du jour, a novel highly pathogenic influenza may be the next severe global health security crisis that the communities are not fully prepared for even with existing strategies and plans.

Departmental Pandemic Planning

The existence of strategies and plans does not always translate into successful and maintained planning and preparedness. In August 2014, the Department of Homeland Security (DHS) Office of Inspector General (OIG) issued a report entitled "DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures" (OIG-14-129). The audit reviewed the internal preparedness of DHS and its components to continue their mission essential functions during a pandemic threat. DHS OIG found that:

> *DHS did not adequately conduct a needs assessment prior to purchasing pandemic preparedness supplies and then did not effectively manage its stockpile of pandemic personal protective equipment and antiviral medical countermeasures. Specifically, it did not have clear and documented methodologies to determine the types and quantities of personal protective equipment and antiviral medical countermeasures it purchased for workforce protection. The Department also did not develop and implement stockpile replenishment plans, sufficient inventory controls to monitor stockpiles, adequate contract oversight processes, or ensure compliance with Department guidelines. As a result, the Department has no assurance it has sufficient personal protective equipment and antiviral medical countermeasures for a pandemic response. In addition, we identified concerns related to the oversight of antibiotic medical countermeasures.*

DHS OIG made 11 recommendations to improve the efficiency and effectiveness of the department's pandemic preparations for which DHS concurred with the intent of all of them.

In January 2016, DHS OIG released an audit report regarding the department's response to the 2014 Ebola virus outbreak. The audit found that DHS components did not ensure that all personnel received adequate training on the passenger screening process or the use of certain protective equipment. The report identified 10 recommendations for the department and its components.

In October 2016, DHS OIG released a follow-up report, entitled "DHS Pandemic Planning Needs Better Oversight, Training, and Execution," OIG-17-02). The report identified progress in planning and preparedness from the 2014 audit, but stated that DHS cannot be assured that its preparedness plans can be executed effectively during a pandemic event. The 2016 audit found:

- Components' pandemic plans did not meet all department requirements;
- DHS pandemic personal protective equipment planning guidance and oversight needs improvement; and
- DHS pandemic reporting and exercising requirements need additional oversight.

This 2016 DHS OIG report identified seven recommendations to improve oversight, readiness, timeframes, training, and exercises. These audits regarding the preparedness of a major federal department bring into question the status and relevancy of previous comprehensive national strategies for pandemic preparedness and the progress truly achieved and maintained after many different global public health threats.

Broader Pandemic Strategy & Planning

There have been numerous essential national strategies, plans, and policies issued in the past decade, many to address the most recent outbreaks or evolving public health concerns. Two of the most notable and foundational documents may be the "National Strategy for Pandemic Influenza" (2005) and "National Strategy for Pandemic Influenza – Implementation Plan" (2006). These documents are important due to their broad focus and wide inclusion of international, federal, state, tribal, local, and private sector partners for a threat that is likely to have the greatest global impact.

©iStock.com/AlpamayoPhoto

The Implementation Plan identified more than 300 critical actions and requirements to address the threat of pandemic influenza. It is unknown how many of these actions and expectations continue to be priorities

and implemented at this time. Many of the actions have been re-identified in subsequent strategies, policies, plans, and after action reports for the emerging and evolving pathogens since 2006. However, a review of many after action reports, studies, and hearings indicates that there remains significant room for improvement in planning and preparedness.

Beyond what has been identified in the previous DHS OIG audits for one department, there are various critical actions that merit review and discussion for the entire nation. In Chapter 8 of the Implementation Plan, entitled "Law Enforcement, Public Safety and Security," the following was stressed:

> *If a pandemic influenza outbreak occurs in the United States, it is essential that governmental entities at all levels continue to provide essential public safety services and maintain public order. It is critical that all stakeholders in State and local law enforcement and public safety agencies, whose primary responsibility this is, be fully prepared to support public health efforts and to address the additional challenges they may face during such an outbreak. Federal law enforcement and military officials should be prepared to assist in a lawful and appropriate manner, and all involved should be familiar with the established protocols for seeking such assistance and have validated plans to provide that assistance.*

To support this priority, there are specific actions, with numerous sub-actions, that require a candid assessment of the status and readiness for a serious pandemic threat such as:

- *8.1.1. Develop federal implementation plans on law enforcement and public safety, to include all components of the federal government and to address the full range of consequences of a pandemic, including human and animal health, security, transportation, economic, trade, and infrastructure considerations. Ensure appropriate coordination with state, local, and tribal governments.*
- *8.1.2. Continue to work with states, localities, and tribal entities to establish and exercise pandemic response plans.*
- *8.1.3. Provide guidance to individuals on infection control behaviors they should adopt prepandemic, and the specific actions they will need to take during a severe influenza season or pandemic, such as self-isolation and protection of others if they themselves contract influenza.*
- *8.1.4. Develop credible countermeasure distribution mechanisms for vaccine and antiviral agents prior to and during a pandemic.*
- *8.3.1. Encourage all levels of government, domestically and globally, to take appropriate and lawful action to contain an outbreak within the borders of their community, province, state, or nation.*
- *8.3.2. Determine the spectrum of infrastructure-sustainment activities that the U.S. military and other government entities may be able to support during a pandemic, contingent upon primary mission requirements, and develop mechanisms to activate them.*

In other areas of the Implementation Plan, critical actions and requirements, with numerous sub-actions, are identified for critical infrastructure, border control, containment, quarantine, and isolation responsibilities:

- *4.1.7. Develop credible countermeasure distribution mechanisms for vaccine and antiviral agents prior to and during a pandemic.*
- *4.2.5. Develop and exercise mechanisms to provide active and passive surveillance during an outbreak, both within and beyond our borders.*
- *4.2.7. Develop screening and monitoring mechanisms and agreements to appropriately control the movement and shipping of potentially contaminated products to and from affected regions if necessary, and to protect unaffected populations.*
- *4.3.1. Work to develop a coalition of strong partners to coordinate actions to limit the spread of a virus with pandemic potential beyond the location where it is first recognized abroad in order to protect U.S. interests.*
- *4.3.2. Where appropriate, use governmental authorities to limit movement of people, goods, and services into and out of areas where an outbreak occurs.*
- *5.3.1. Encourage all levels of government, domestically and globally, to take appropriate and lawful action to contain an outbreak within the borders of their community, province, state, or nation.*
- *5.3.2. Where appropriate, use governmental authorities to limit non-essential movement of people, goods, and services into and out of areas where an outbreak occurs.*
- *5.3.4. Provide guidance to activate contingency plans to ensure that personnel are protected, that the delivery of essential goods and services is maintained, and that sectors remain functional despite significant and sustained worker absenteeism.*
- *6.1.13. Develop credible countermeasure distribution mechanisms for vaccine and antiviral agents prior to and during a pandemic.*
- *6.3.1. Encourage all levels of government, domestically and globally, to take appropriate and lawful action to contain an outbreak within the borders of their community, province, state, or nation.*
- *6.3.2. Provide guidance, including decision criteria and tools, to all levels of government on the range of options for infection control and containment, including those circumstances where social distancing measures, limitations on gatherings, or quarantine authority may be an appropriate public health intervention.*

The few actions listed above demonstrate the enormous undertaking for the public sector to plan and prepare for a highly pathogenic pandemic influenza or other significant public health threat. It is unknown when all of these actions were last fully reviewed and evaluated by the identified and responsible departments, agencies, and organizations. It is an extremely important question to have answered. Fortunately, nongovernmental organizations and other private sector partners continue to support and fund the planning and preparedness for epidemics and pandemics.

Private Sector Collaboration

In August 2016, the Coalition for Epidemic Preparedness Innovations (CEPI) was founded in the United Kingdom at the Wellcome Trust Headquarters. CEPI is collaboration between the Wellcome Trust, the Bill and Melinda Gates Foundation, the World Economic Forum, and the government of Norway to prepare the world for future outbreaks of disease.

In September 2016, the Blue Ribbon Study Panel on Biodefense announced that it received over a million dollar grant from the Open Philanthropy Project to continue assessing the nation's biodefense systems, issuing recommendations and advocating for their implementation, and informing policymakers and lawmakers on viable avenues for needed change. In the same month, Mark Zuckerberg and his wife Priscilla Chan announced that they planned to invest at least three billion dollars in the Chan Zuckerberg Initiative over the next decade to focus on preventing, curing, and managing all diseases by the end of the century.

In October 2016, the Trust for America's Health released the "Blueprint for a Healthier America 2016: Policy Priorities for the Next Administration and Congress." The report identified key strategies for improving the health of Americans through a new approach to health by prioritizing improving health and addressing major epidemics in the United States.

Although not a truly private sector organization, the World Bank created the Pandemic Emergency Financing Facility to provide funds during outbreaks of specific infectious diseases to become more actively engaged in pandemic preparedness and response.

An Honest Assessment

The involvement of influential private foundations, initiatives, and organizations is essential for this monumental planning and preparedness tasking. They are crucial partners for success and leadership. However, the need for thoughtful, continued, and consistent planning by governmental organizations is just as important for emerging public health and biosecurity threats.

Although dated, the Pandemic Influenza Strategy and its Implementation Plan are two of the strongest frameworks for evaluating the current whole of community preparedness when used to make an honest assessment. The subsequent strategies and plans over the past decade have addressed the most recent specific pathogenic concerns, but they often are quite focused in topic and very frequently forgotten upon the arrival of the next emergence or international incident. There continues to be a necessity for an expansive, inclusive, and implemented strategy for all pandemic threats because a novel highly pathogenic influenza may be the next serious global public health crisis that the nation is not ready for – with massive catastrophic consequences. To be better prepared, these are two critical documents to review, assess, and absolutely update in 2017.

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.

Tomorrow's Emergency Management Capabilities

By Jeffrey Kaliner

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a solid set of guiding principles for homeland security actors to "build, sustain, and deliver core capabilities." Perhaps most important to this process, exercise evaluators assess performance with regard to stated objectives and then identify and document areas of improvement for the tested capabilities.

Evaluators help to identify the gap between where response partners currently are with respect to a given capability and the standard to which they would someday like to achieve. Ideally, in the improvement planning stage, corrective actions are taken to close the identified gaps.

The Known & Unknown

This linear process suggests a predictive capacity with regard to knowable threats and hazards and how they should or could be navigated using certain core capabilities. In other words, capabilities are developed based on the assumption that what worked in the past in one scenario will work again in a future scenario and that these behaviors and actions can be reliably repeated. According to a 2002 article published in the Harvard Business Review, this sensibility has reasonable validity in decision-making contexts that are "simple" or "complicated." In these ordered and predictable domains, history has proven that cause and effect will consistently yield the same results. For example, a Class A fire (ordinary combustible materials) can be easily doused with a water-filled Class A fire extinguisher. Because these results are repeatable over time, the contextual domain can be defined as simple (a straight line between cause and effect) and the term "best practice" has appropriate use because employing this method is indeed truly the "best" response each time.

However, the same assumptions cannot be made about core capabilities in contexts that The Harvard Business Review refers to as "complex" or "chaotic." In these unpredictable and unknowable domains, there are no best or even good practices to rely on. Assuming that basic capability tasks and priorities can be completed in these domains is potentially dangerous. According to the authors, the practices, solutions, or capabilities to address problems or decisions within these contextual frames will be emergent (complex domain) or novel (chaotic domain). An example in this instance would be the "problem" encountered by the Apollo 13 mission in 1970. The crew and support personnel did not train or plan for the incident. All individuals involved needed to improvise with random parts and materials that were already in the craft. In other words, the solution emerged over time because the context was complex and it was only in retrospect that true cause and effect was understood.

A Limited Capability Set

Here lies the limitation with the current homeland security capability model. Capabilities (and plans) are developed with an assumption that they will be operationalized in known and predictable domains. However, it can be reasonably argued that future catastrophic events will be either initiated or influenced by incredibly complex phenomenon. Human beings are not prepared to understand let alone navigate (via existing plans and capabilities) the unintended consequences of a complex array of interacting forces that have been unleashed within the past few decades. Meta-hazards – such as worldwide political unrest, 3-D printed weapons, climate change, fake news, aging populations, automation, artificial intelligence, failing educational systems, globalization, emerging pandemics, and drought – are all indicators of a highly interdependent, connected, and ultimately unpredictable world that will present unknowable future hazards, consequences, and risks for the homeland security enterprise. In other words, although emergency managers plan and prepare for all-hazards, there is no way to conceptualize plans and capabilities needed with regard to the hazards and threats that they will one day face in an increasingly complex future state.

Ultimately, the future is sure to bring threats and hazards that today's emergency response plans and capabilities will fail to adequately address.

In this context, the current capability set (and the methods to improve it) is a somewhat limited solution to an increasingly dynamic and complex set of catastrophic possibilities. This is obviously not to say the current capabilities should be discarded. These capabilities certainly have a place in contexts that are knowable and predictable. It is also reasonable to assume that these capabilities will have use in domains that are unpredictable and unordered (e.g., Apollo 13). However, the future will hold incredibly complex and dangerous problems that current capability sets will be unable to address.

To put it another way, risk management professionals are in the difficult position of navigating two different contextual realities by trying to implement artifacts (capabilities, plans, etc.) produced in one context (pre-event) into that of another that exists in a perceived but ultimately unknowable and unpredictable future dynamic. That is why consideration of an alternative and additional set of emergency management capabilities that will help ready the enterprise for the unknowable consequences of tomorrow's threats and hazards is imperative.

Tomorrow's Emergency Management Capabilities

To ready the enterprise for the unimaginable, emergency managers first need the capability to distinguish between predictable and unpredictable domains. For example, by

being able to apply contextual sense-making tools such as the Cynefin Framework, response professionals are able to consider situational awareness in a new way that assists in solving problems and making decisions. As described in the examples above, an understanding of the difference between static (predictable and ordered) and dynamic (unpredictable and random) contexts can help decision makers to determine if an existing solution or capability will solve the problem or if an emergent or novel solution will be necessary.

Once emergency managers develop the capability to distinguish between different ontological realities, they will need new capabilities to operate within complex and chaotic contexts. Real-time learning, as its own discrete emergency management capability, would set the foundation and stage for navigating within these unpredictable domains. Public Affairs Professor Donald P. Moynihan refers to this ability as "intracrisis learning." There is no doubt that response professionals learn during complex events. An example would be a standard operating procedure that is revised multiple times during a crisis until it truly reflects the intended result. Each revision demonstrates new learning (based on a cycle of action and reflection) that is immediately pushed back into the document in real time. Learning does not wait until the end of the event or exercise but emerges during the actual play. Just like for the crew and support personnel of Apollo 13, this type of emergent and improvisational learning is key to success in navigating chaotic and complex domains.

As it turns out, research suggests that improvisation is an integral part of the learning process in uncertain and complex environments. Thus, a formal and structured improvisation capability would give emergency response professionals another tool to navigate within the unknown. Andrew J. Phelps, Oregon Office of Emergency Management Director, explored the idea of collaborative learning in relationship to improvisation in his Naval Postgraduate School thesis, entitled "Play Well With Others: Improvisational Theater and Collaboration in the Homeland Security Environment." Phelps recommends that homeland security practitioners be trained in improvisational

techniques to enhance collaboration. He also suggests that an improvisational model could be used to evaluate collaboration during the after-action review process.

Using this type of alternative methodology to evaluate complex human interactions makes sense. The traditional after-action review process relies on a simple and linear set of questions and practices that cannot truly capture the dynamic complexity of modern exercises and events. Just as new response capabilities are needed, so is a new set of capabilities and techniques to help elicit, develop, and capture the knowledge generated during an event or exercise.

Appreciative inquiry is one such existing technique: a type of action research that deliberately asks participants positively framed questions that are focused on the foundational strengths and accomplishments of the past to craft innovative and collaborative futures. Participants are encouraged to share their responses through constructive dialogue and storytelling to capture the nuances, richness, and complexity of their shared and interconnected experiences. Appreciative inquiry assumes that complex problems (such as multiagency emergency response) cannot be understood or solved by traditional linear methods or models. In other words, perceiving a multiagency intervention within a traditional problem-solving methodology (how to "fix" what is "broken") cannot fully consider the complex adaptive system at the heart of any interdependent emergency response.

Beginning the Discussion

Ultimately, the future is sure to bring threats and hazards that today's emergency response plans and capabilities will fail to adequately address. The reality is that nobody will ever be able to produce all the capabilities needed for every possible disaster scenario. Thus, beginning the conversation now on how to create and develop additional individual and organizational capabilities that will allow for real-time learning, improvisation, innovation, and adaptation based on an understanding of contextual sense making is critical. The increasing complexity of modern-day exercises and emergencies demands that response agencies have an alternative capability set. If not, emergency management professionals will forever be one step behind when trying to navigate the consequences of the threats and hazards of tomorrow.

Jeffrey Kaliner is a homeland security instructor at Cascadia Technical Academy in Vancouver, Washington. Before his current position, he served as an emergency preparedness liaison for the state of Oregon and, before that, he helped build the City of Chicago's Bioterrorism Preparedness Program by serving as its first director of training and education. He holds a Master of Arts degree in security studies from the Naval Postgraduate School and a Master of Science in education from Northern Illinois University.

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