domestic preparedness .com

DomPrep Journal

Subscribe Volume 11 Issue 5, May 2015

Call Center

IntegratiOn

TelecomMunication

ManageMent Software

PUblic Sector

Mass Notification

InteroperabIlity

Business Continuity

PrivAte Sector

ThreaT Analysis

ElectronIc Data

sOcial Media

FirstNet

Since 1998, Integrating Professional Communities of Homeland Security, Preparedness, Readiness, and Resilience

RADIATION DETECTION & IDENTIFICATION

SMALL. SIMPLE. SPECIFIC.

Confident decision-making is critical when lives are at stake. Emergency responders must have fast and accurate threat information where they need it the most - in the field.

FLIR is focused on delivering advanced threat detection and identification tools that are more affordable and easier to use than ever before.

For example, the identiFINDER® R300 is the world's first pager-size radiation instrument that can detect, locate and identify radioactive isotopes.

Worn on a belt similar to a personal radiation detector (PRD), the identiFINDER® R300 provides the operator with all the information necessary to respond with confidence in the most hazardous and stressful environments.

To learn more about the identiFINDER® R300 and our other laboratory-caliber products visit www.flir.com/r300

FLIR®

THE WORLD'S SIXTH SENSE™

/flirhq @FLIRdetection

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

James D. Hessman
Editor Emeritus
JamesD@domprep.com

Catherine Feinman
Editor
cfeinman@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

John Morton
Senior Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, 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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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: When Alexander Graham Bell patented the telephone in 1876, it is unlikely that he could predict how much communication would evolve over the next 139 years. With the cord cut from most modern communication devices, technology offers many new avenues to communicate, but with each advancement comes new privacy and security concerns. (Photo by iStockPhoto)

Editorial Remarks

By Catherine Feinman

The topic of communications covers everything from a face-to-face meeting to hidden cyber messages on the Deep Web. The May issue of the DomPrep Journal tackles this broad topic and weaves together the different perspectives with the common goal of ensuring effective, timely, accurate, and secure information. Steve Cohan leads this issue with a peek into the future of communications interoperability. He shows how gaps can be closed and hurdles overcome when public safety agencies carefully and collaboratively plan to keep lines of communication open during both normal and emergency operations.

Charles Werner describes the situational and operational awareness benefits of including the National Information Sharing Consortium to operationalize capabilities, create dialogue, and close communication gaps. Similarly, Janusz Wasiolek shares a case study of how the greater Phoenix area used the Homeland Security Information Network as a tool to communicate between public safety officials tasked with managing multiple events simultaneously.

During large-scale events and disaster incidents, the public wants to know what is happening. As technologies change, information-sharing techniques must adapt to the new information-sharing environment. Anthony Mangeri defines what it means to work with the mass media – as allies or adversaries – in today's world.

Regardless of the specific technology or method employed, some lines of communication must be protected and secured. Anyck Turgeon describes the ethical and not-so-ethical cybercommunications environment. She emphasizes the importance of understanding the open and hidden world of cyber in order to fortify emergency response, disaster recovery, and business continuity efforts.

InfraGard is one public-private partnership that helps protect the United States from credible threats. By incorporating sector chiefs within each chapter, as described by Sheri Donahue, the Federal Bureau of Investigation and InfraGard members and can rapidly share and disseminate necessary critical information.

Rodrigo Moscoso highlighted one recent example of a failure in effective public-private communication: A mailman from Florida breached restricted airspace over the nation's capital and landed a gyrocopter on the West lawn of the U.S. Capitol building. Although not a surprise, it did surprise law enforcement authorities. Fortunately, this incident ended peacefully, but the next one may not.

Rounding out the issue are the results from a survey that DomPrep conducted in line with this month's communication theme: "Bridging the Public-Private Sector Divide." Beginning with an idea at a local business continuity meeting, people from across the United States, Canada, and Martinique shared their public and private sector perspectives on how to encourage private sector businesses and organizations to develop continuity plans, which in turn would create more resilient communities.

What the Future Holds for Communications Interoperability

By Steve Cohan

The terrorist attacks of 9/11 put a spotlight on the gaps that existed and, in many jurisdictions, still exist between public safety agencies. Although most preparedness professionals would agree that it is critical to have interoperable communications, there are factors that hinder achievement of this goal. With careful consideration, agencies can overcome these hurdles.

Since the tragic events of 9/11 as well as numerous other events when communications were disrupted, a popular topic of conversation among first responders has been communications interoperability, which is the ability to use radio systems from one jurisdiction to another or from one discipline to another without the need for technical adjustments. It is the ability simply to be able to talk to each other. Unfortunately, this vision has not yet been fully realized. In every desktop or deployed exercise this author has participated in, communications always arose as the number one issue in terms of exercise performance.

Technical, Political & Cost Hurdles

There are a number of reasons why this vision has not been realized. Some are technical in nature and some are for political and cost reasons. Cost requires no explanation since radios and systems are, in a word, expensive. Part of the reason for that is that most modern radios are more sophisticated and many now even have IP addresses, just like computers. Additionally, with the advent of data capabilities such as texting, geolocation, and handset remote control, these features simply cost more. Owing to the sophisticated nature of these radios, licensing of the onboard software (firmware) add to the cost. Add to that the fact that wide-area coverage requires more towers, need for simulcasting, and need for computer-aided dispatch (CAD) interoperability, and such interoperability becomes a very expensive prospect.

In addition, the "laws" of radio frequency do not change. So, frequency choice is a major consideration that ultimately affects interoperability. In the mountain states, VHF is the usual choice. On flat terrain, UHF or 700/800 MHz is the usual choice. Each frequency has different benefits and characteristics. VHF tends to "bend" around geographic topology such as hills, whereas the higher the frequency (700/800 MHz), the less radio waves bend making operations more line-of-site. Although higher frequencies tend to penetrate buildings better, they require more towers for line-of-site operation. The ability of digital computer-driven systems currently available for 700/800 MHz have the benefit of being able to handle large amounts of traffic as well as field unit control.

Site traffic also plays a part in choosing the right system and having a better ability to have interoperability. The more traffic on any given tower, the more chance that tower can become overloaded, thus denying users access.

Lastly, there are always political considerations. Most of these derive from prejudices concerning brands of radios or systems, cost, or vendor relationships.

Legacy vs. Emerging Systems

Because there are still legacy systems – both analog and digital – that are currently deployed as well as disparate radio and system types, panel patching and gateways have been popular to bridge networks to create an interoperable environment. When systems are working well and systems and people are not stressed, the ability to communicate among systems works well. But, like anything technical, under duress, physical destruction, lack of personnel to deploy systems, etc., some technologies may not work or may not work well. In other words, the more complex the system, the more chance for breakage. Some radios allow for "simplex" operation – that is, handheld-to-handheld communications without the need for repeaters or gateways, but the range is limited to line-of-site and these radios only work on the same frequency with the same modulation type.

New to this hodge-podge of radio systems is the need for data and visual communications (video streaming), which further add to the considerations for designing and implementing radio systems. A relative newcomer to all of this is FirstNet. FirstNet's model is long-term evolution (LTE) 700/800 MHz on handheld devices similar to today's current smartphones, the purpose of which is to be able to transmit various data types but do so on a network dedicated to first responders. This system is different than the traditional land mobile radio (LMR) systems. Inasmuch as this system is still under development with a few deployed test beds – such as the one in Adams County, Colorado – much work still needs to be done, especially in the area of site deployments.

In the end, the system will look similar to current cellular systems deployed by the four major carriers in the United States. It should be noted that wide-area coverage would no more likely be attained than current cellular systems give geographic and cost issues. Some first responders have expressed concerns that they would now be required to carry another handset along with their LMR radios and their cellphones. Eventually, more fully featured radios may solve this issue with combination cost-effective LTE/LMR radios but that is a ways off if it ever actually becomes reality.

Future Considerations

Secondary considerations for system uptime include disturbances like electromagnetic pulse – or electromagnetic pulse disruptions or damage. These can happen from three general sources: (a) the sun with geomagnetic storms; (b) nuclear explosions; or (c) adverse pulse weapons events causing physical destruction. Should one of these events take place, the power grid itself could be damaged, as could radios, computers, antenna systems, routers, and so forth. Many of the current public safety radio systems are not adequately hardened to mitigate or prevent these kinds of destructive events. As such, these systems obviously would have a material impact on the ability to communicate via radios and have an effect on the power grid system, thus denying power to many communications centers or other radio systems, as described in the U.S. Department of Energy's Quadrennial Energy Review.

It appears that in the next ten years or so, console patching and gateways will become the mainstay of interoperable public safety communications. There are simply too many disparate systems, radios, and – most importantly – needs for any one solution be the ultimate solution. Although these systems generally perform as expected, it would behoove every agency to consider alternative methods of communications should there be primary system failures. In other words, "You can never have enough arrows in the quiver if you intend to survive … and communicate."

Steve Cohan is currently the national coordinator for the Joint Communications Task Force (JCTF), vice chair of the Federal Bureau of Investigation (FBI) InfraGard National Electromagnetic Pulse-Special Interest Group (EMP-SIG), and vice president of the Board of Directors for FBI InfraGard Denver. He has served 44 years in law enforcement and public safety in a variety of positions including patrol, investigations, communications, administration, and training. He has served with the JCTF and its predecessor for over eight years. The JCTF was originally conceived and operated within the City & County of Denver Police Department and Combined Communications Center, and has since become a national organization. His expertise is in the area of law enforcement, communications, and information technology.

How to Deploy an Ethical Cybercommunications Program

By Anyck Turgeon

Cybercommunications 101: How to deploy an effective cybercommunications program as part of an emergency, disaster recovery, and business continuity effort. As more common, daily-use devices become automated, the risk of cybersabbotage and cyberattacks increases, so planners must take measures to prevent harm to their efforts, personnel, and agencies or organizations.

> *"The victorious make many calculations prior to the fight,*
> *for every battle is won before it is ever fought."*
> –Sun Tzu, ca. 2nd century B.C., Book: *The Art of War*

As emergency personnel deal with a larger amount of threats (including shutdown or takeover by hackers of their communication tools) and as companies reach farther into global markets where cybercommunications are critical, everyone must comply with a much larger spectrum of barriers – for example, international regulations (particularly Foreign Account Tax Compliance Act, privacy, and cybersecurity laws). To understand how to develop and deploy a cybercommunications plan, one must appreciate its importance, different attributes, and complexity.

Crisis Communication vs. Cybercommunications

From the devastating explosion of a chemical plant in West, Texas, to wildfires in California or an ice storm in Montreal, Canada, emergency personnel are fledged at crisis communications. Yet, given the speed and scale of replication of cybercommunications, it is important to study, learn, plan, and adapt to this newer, critical tool that can easily be turned into a weapon.

On 20 May 2015, the Office of the Director of National Intelligence released more than 100 declassified documents that were captured after the U.S. presidential order to kill Osama bin Laden. Those documents revealed that food security was considered an essential good for survival by terrorist groups like al-Qaida. Similarly, cybercommunications must be treated as a critical element of any emergency planning, response, and recovery effort. To ensure the survival of all parties involved, emergency personnel must consider the exponentially more efficient qualities of cybercommunications as well as its dual nature.

Unlike standard crisis communications, whereby there is a specific order in what gets communicated to certain communities, cybercommunications are distributed universally and, when intercepted, can distribute various decentralized news, information, instructions, and orders. When developing cybercommunications programs, planners should consider the exponentially super-size scale, speed, tight coupling, decentralized and multilayer technological architectures, distribution, and opacity of cybercommunications.

The Fragility & Impact of Cybercommunications

As cyberbullying is on the rise, with one in three teenagers now tormented, humiliated, threatened, and even led to suicide from targeted and hacked cybercommunications, it is important to understand the potentially destructive and disabling nature of this progressive, more pervasive, and modern communications approach. For example, in a recent case in Leander, Texas, a 9-year-old cyberbully by the name of Jaide was able to take over Instagram, Facebook, and cellphone text communications of her targets as well as gain access to all Internet communications from a hacked Time Warner box (including access to all security cameras and digital transmissions). In order to rid themselves of the death threats, compromised cybercommunications, and defamatory digital defacing, the families of the targeted cybervictims had to entirely change all of the cybercommunication devices and terminate social media profiles.

On a grander international scale, cybercommunications are now often hacked to disable larger communities through chaos. Since the initial disruptive attacks by the Morris worm in 1988 (resulting in the first cybercommunication convictions under the U.S. Computer Fraud and Abuse Act), disruption of cybercommunications is being used as a standard preemptive method of massive dehabilitation prior to physically violent manmade attacks. Famous examples of this cybercommunications phenomenon include:

- The 2007 attacks in Estonia, which disrupted government services, halted online banking, and disrupted cybercommunications;
- A March 2015 blackout by Iranian cyberhackers, which paralyzed Turkey; and
- Recent cyberhacking pledges over the Deep Web, which report plans of future cybercommunication blackouts by the Islamic State group.

In fact, in its published history of cyberattacks, the North Atlantic Treaty Organization (NATO) has reported over 18 incidents when countries like Canada, China, Israel, South Korea, and the United States were impaired without cybercommunications prior to acts of war.

Cybercommunications – Helping or Impairing Emergency Personnel

As people and resources around the world can receive information up to a speed of the nanosecond, cybercommunications definitely can empower users. Modern societies are moving toward the "Internet of Things," which is defined as a network of physical objects or things embedded with electronics, software, sensors, and connectivity that enable these objects to achieve greater value and service by exchanging data with the manufacturer, operator, and/or other connected devices.

In addition, communications are being anonymized via the Deep Web (aka Deepnet, Invisible Web, or Hidden Web), which is defined as the 96-percent portion of World Wide Web content that is not indexed by standard search engines and cannot be accessed through common browsers like Microsoft Internet Explorer or Firefox. This brings up an important point that most emergency personnel rely on four percent of the more common and most hacked Internet for their cybercommunications. As a result, simple devices like employee cars, microwaves, or modern refrigerators with computerized management and cybercommunication capabilities can now be disabled, or turned into lethal weapons.

As time and safety are the essence of emergency services, having an emergency vehicle suddenly stop moving, or even explode, as a result of hacked cybercommunications would be an eye opener to many. All digitally enabled devices, by design through network layers and transportation protocol, now can be used to disable, counter, or even terminate efforts, critical personnel, and organizations.

The Good, the Bad & the Ugly

In 2010, a shooting took place at the University of Texas. Confidential security communications from emergency personnel was intercepted by cyber pundits and redistributed to the media for mass distribution. As the university police personnel communicated their limited capacity to counter the attack, they asked for assistance from Austin Police Department and other related agencies. Colton Tooley, a 19-year-old mathematics major, was firing AK-47 shots from an upper floor of the Perry-Castaneda Library, but the guns used by the university police did not have the necessary range to disable the shooter.

Unfortunately, the confidential communications were breached, sensationalized, and enhanced when redistributed. Journalists asked the public to drop by the University of Texas campus and start shooting the vaguely disclosed source of the shooting with their own personal firearms. As a result, hundreds of concealed handgun license carriers showed up and began free-range shooting. With bullets bouncing back from various buildings, emergency personnel had to deal with an army of unmanaged shooters trying to be good citizens and save the day. Although the propagation of cybercommunications was not as pervasive as it is today, the bad attributes of cybercommunications rapidly bypassed the positive ones – even with well-intentioned citizens.

Automation of intelligent devices through potentially breached to manipulated cybercommunications has the capability and very likely outcome of adding a multiplying factor to good and bad cybercommunications.

Preventing or Limiting Misuse of Cybercommunications

Although the topic of cybercommunications could fill several books, a good start is to include cyberethics as part of any cybercommunications program. Cyberethics is a modern discipline that encompasses: digital user behaviors; tasks that computerized devices are programmed to do; and effects on individuals and society.

Just like ethics were derived from the German Nuremberg Doctors WWII trial and resulted in the 1947 Nuremberg code (whereas scientific experiments conducted on humans need to adhere to a code of ethics) as well as the 1964 Declaration of Helsinki, cyberethics emerged upon the deployment of the National Research Act of 1974. This suite of developments gave birth to the

1981 Belmont Report and the 2012 Menlo Report. Through a framework called “Common Rule,” the 2012 Menlo Report is now more commonly used to govern and assist decision makers with ethical standards in information and communication technology.

As much as these two reports focus on computer security research – for example, how to stop botnets that are affecting millions of humans by damaging systems and data in foreseeable, yet nearly unpredictable, patterns – the following focus areas of cyberethics to be applied upon cybercommunications should be considered during any emergency, disaster recovery, and/or business continuity effort:

- Understanding the different characteristics of cybercommunications versus standard communication methods;
- Ensuring respect of persons (identification of stakeholders – primary, secondary, and key participants, as well as securing informed consent);
- Fostering beneficence (distribution of risks, benefits, and burdens starting with identification of potential harms versus benefits including: integrity risks, availability risks, confidentiality risks, necessary secrecy, and transparency, plus mitigation of realized harms);
- Promoting justice (fairness and equity); and
- Respecting law and public interest (compliance, transparency, and accountability).

U.S. Laws Governing Cybercommunications

Although compliance does not ensure security and privacy, some of the U.S. laws that corporate executives, board members, as well as emergency, disaster recovery, and business continuity professionals may want to familiarize themselves with upon planning, designing, implementing, and testing a cybercommunication program include:

- The Communications Act of 1934 (as amended by the Telecom Act of 1996), 47 U.S.C. § 151 et seq.
- The Communications Act of 1996, Protection of Customer Proprietary Network Information, 47 U.S.C. § 222
- The Electronic Communications Privacy Act – Wiretap Acp, 18 U.S.C. § 2510-22
- The Stored Communications Act, 18 U.S.C. § 2701-2712
- The Pen Register & Trap/Trace Act, 18 U.S.C. § 3221-27
- The Telephone Records and Privacy Protection Act, 18 U.S.C. § 1038
- The Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g(a)(4)(A)
- The Health Insurance Portability and Accountability Act of 1996, Pub. Law 104-191
- The Privacy Act of 1974, 5 U.S.C. § 552a(a)(5), (a)(4)

Ensuring the availability, integrity, security, resilience, and reliability of an organization's cybercommunications infrastructure and activities can be intimidating and challenging. U.S. and foreign organizations are invited to review the tools provided by U.S. Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate. With the primary objective of protecting federal communication networks since 2006, CS&C carries out its mission by engaging the private sector in a collaborative manner through its five divisions:

- The Office of Emergency Communications
- The National Cybersecurity and Communications Integration Center
- Stakeholder Engagement and Cyber Infrastructure Resilience
- Federal Network Resilience
- Network Security Deployment

A Final Key Element: Contextualization of Cybercommunications

Cybercommunications are already catapulting and "taking over the world." More comprehensive cybercommunication programs are required that include extensive cyberethics from conceptualization to deployment and testing. Another important topic of cybercommunications planning is contextualization, which is defined as the intelligent aggregation of independent data, signals, and metadata from all layers of the Open Systems Interconnection (OSI) model. Contextualization enables the overwriting of malicious code being pushed (through Wi-Fi network as unauthorized to write at the physical signal level) that can disable an emergency vehicle, take over a cybercommunications network, and turn the vehicle into a lethal weapon through disabled brakes, forced fires (combustion through disablement of cooling systems), or constructed explosions (via overheating, melting, and heat explosion).

> ***"Simple devices like employee cars, microwaves, or modern refrigerators with computerized management and cybercommunications capabilities can now be disabled, or turned into lethal weapons."***

Cybercommunications can become a phenomenally powerful and empowering tool as well as a weapon of war. It is interesting how the Internet was originally designed with the intent to be an equalizer. Yet, as they are progressively becoming more lethal, cybercommunications are now a critical differentiator – especially in times of emergency.

With more than 25 years of technology innovation and security experience, Anyck Turgeon (CFE, GRCP, CRMP, CBA, CCIP, CHTI, SMIA, CEFI, CDS, EP, C:CISO) is a proven cybersecurity, fraud, and money laundering data scientist helping individuals, corporations, and governments with their cybercommunications needs. With more than 25 years of experience, she currently leads M-CAT Enterprises and The Fraud Institute, works as a principal analyst at Eckerson Group as well as serves as an advisory board member at the Association of Certified Fraud Examiners (ACFE), McKinsey, University of Texas – Butler School Of Music, Door64, and Firestorm Solution. For more information, contact the author at Anyck@mcatenterprises.com

Critical Elements for Creating a Dialogue

By Charles Werner

Accessing and sharing information between various agencies and organizations may be challenging, but are necessary for developing effective situational and operational awareness. In June 2012, the National Information Sharing Consortium (NISC) formalized an approach for such interagency communication. By operationalizing these capabilities, NISC creates dialogue and closes communication gaps.

Data and information sharing are critical elements to understanding and enhancing a community's resilience. The first step is to identify a normal baseline of daily life/activities in a community. Defining a baseline is important because it provides the norm, which can be compared to a new activity level caused by a natural or manmade disaster – for example, incidents, power outages, storm surge, road closures, and evacuations. Today more than ever, a diverse dataset is available from local, state, and national/federal sources to help understand the norm and to measure against the new activity level. To this end, the NISC in cooperation with the Incident Management Information Sharing Subcommittee is working on the development on a list of essential elements of information that have been reviewed by numerous incidents and training exercises as a starting reference point.

This knowledge combined with available and affordable technology provides near real-time situational awareness that can be readily shared with other people and other organizations simultaneously without relying on voice technology. As a result, situational awareness may be updated and monitored by tribal, local, state, federal agencies, and national organizations in order to know: (a) what is happening; (b) where it is happening; and (c) the magnitude of the situation. This then can facilitate the process of moving forward with resources to assist the impacted area.

Categorizing Critical Properties

The successful utilization of data is based on several factors, including: governance, standard operating procedures, data, training, and usage. The process may likely begin with data discovery or learning what data is available from various sources (local, state, and national) and then how this data can be used to recognize a community's situation – for example, daily normal stats, increased emergency responses, and catastrophic events. Many people and organizations are not even aware of the vast amount of information and geospatial data that is available and accessible at the local level, or how this information can be related to normal versus unusual situations. A tip for local responders is to begin a dialogue with the local geographic information system coordinator to share information needs, to identify available information, and to determine how the information can be accessed and used.

The Department of Homeland Security (DHS) SAFECOM Interoperability Continuum can be used to provide a template to guide effective information sharing processes, the critical elements properties of which are categorized by the following "lanes":

- *Governance* identifies oversight and defines roles and responsibilities necessary for information sharing.
- *Standard operating procedures* define what, when, and how information will be shared and with whom.
- *Training and exercises* are required to ensure that all involved know how to effectively share the information.
- *Usage* becomes most relevant or applicable when the process of information sharing or exchange is used on a daily basis and transforms situational awareness into daily operational awareness. Operational awareness then becomes the norm and establishes an organization's or locality's baseline from which to better understand the impact that a significant event or emergency incident is having on the organization or locality.
- *Technology* (data and voice) is addressed last because of the criticality of data and the determination of what technology is needed.

How data is managed, organized, and published ultimately determines how effectively information can be shared. Once the other lanes of the continuum have been addressed, use of data can be most productive when it exists in a standardized data format and is managed within a common and shared data folder architecture and common symbology (for geospatial visualization). When the data lane is clearly identified, accessible, and in the right format, it simplifies how information can be shared and enhances the way it can publish, access, consume, and share the information through various technologies.

> ***"A reliable flow of information between all of these agencies and organizations is required to respond to and mitigate both daily emergency incidents and catastrophic natural and manmade disasters."***

Information Sharing & Incident Management

The National Information Sharing Consortium (NISC) was organized to identify the necessary steps for developing an effective information sharing environment. National security data is growing in volume and complexity almost daily, challenging end users to screen applicable as well as any unnecessary data and information. Stakeholder input, participation, and collaboration are needed so government at all levels can identify and categorize threats (both natural and human caused) and effectively mitigate or respond to incidents when needed. A rigorous approach is needed to establish critical information sharing requirements, which would help frame standards-based approaches for both information sharing and incident management. The NISC is dedicated to addressing this critical endeavor and bases its initiatives and activities on a coordinated approach that validates needs and requirements, minimizes culls emerging gaps, promotes best practices, maximizes situational/operational awareness capabilities, and influences policy and grant guidance (see Figure 1).

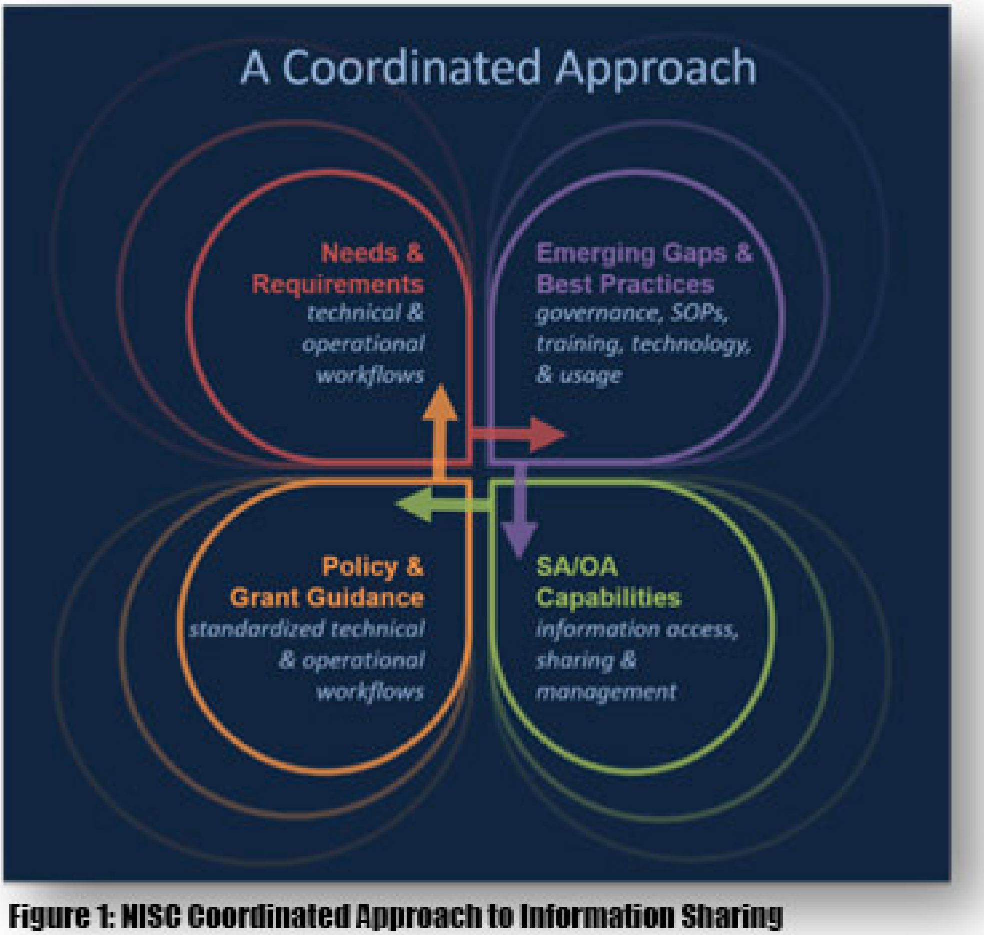


Figure 1: NISC Coordinated Approach to Information Sharing

The organization’s leadership has been working with leadership of the DHS Science and Technology Directorate (DHS-S&T) and the White House program manager for the information sharing environment by co-chairing an advisory body – the Incident Management Information Sharing Subcommittee (IMIS-SC) – to develop a national strategy on information sharing. This strategy would help to standardize how information is shared between public safety disciplines, public service, all levels of government, nongovernmental organizations, and the private sector. A reliable flow of information between all of these agencies and organizations is required to respond to and mitigate both daily emergency incidents and catastrophic natural and manmade disasters. The IMIS-SC’s focus is described in its charter as follows:

> “To address the information sharing needs of federal, tribal, state, and local emergency management sectors, the White House Information Sharing and Access Interagency Policy Committee (ISA-IPC) has chartered the Incident Management Information Sharing Subcommittee (IMIS-SC). The IMIS-SC will provide guidance and policy recommendations to the ISA-IPC – from local, state, federal

> and industry perspectives – on ways to both expand and institutionalize nationwide incident management information sharing capabilities and system interoperability across the homeland security enterprise."

The NISC also is taking a focused look at information sharing needs at the local level, specifically from the first responder perspective. The NISC was awarded a DHS Information Sharing grant in support of its "Local First Responder Information Sharing Decision Implementation Project" – a series of technical assistance engagements involving exploration of day-to-day operational needs within and across public safety disciplines. Emphasis will be placed on methods for managing information to enable informed decision making at every point in the chain of response. This would further include: (a) points that require state-level involvement; and (b) development of an information sharing model that can be replicated.

Building Capacity at the State & Local Levels

Using the NISC's coordinated approach, lessons learned and best practices from all its engagements and activities would inform the establishment of an information sharing environment that maximizes access to nationally relevant data. Access to this data would be accomplished in a multitude of ways, using a variety of technology tools that support publication, management, and sharing of data products. This would include but not be limited to aggregated web maps, applications, and direct access to data libraries. These efforts are conducted in partnership with DHS S&T as S&T's transition partner for the Virtual USA® Program – a program that is focused on building capacity of state and local agencies' incident management communications and information sharing capabilities. S&T's ongoing national leadership role in advancing information sharing among all levels of government and the private sector underscores the critical importance of this partnership for helping the NISC reach its goals.

The NISC now has more than 100 local, state, and international organizations as members, and it continues to expand. For more information about the NISC, the NISC Portal (powered by ESRI ARCGIS Online), as well as how to join (its free for the public sector) and to get involved, visit the website at http://www.nisconsortium.org

Charles Werner is a 41-year veteran of the fire-rescue service who now serves as Chair of the National Information Sharing Consortium, Board of Directors for National Alliance for Public Safety GIS, and Co-Chair of the White House/U.S. Department of Homeland Security's Incident Management Information Sharing Subcommittee. He can be reached at wernerc@charlottesville.org

Football, Golf & an Integrated Public Safety Information Network

By Janusz Wasiolek

Managing one large-scale special event can be a public safety challenge for any jurisdiction. However, when multiple events and hundreds of thousands of people converge in one area, communications between public safety officials is critical. Using the Homeland Security Information Network, officials in the greater Phoenix area kept the lines of communication open.

From New Year's Eve through 2 February 2015, the greater Phoenix, Arizona, area hosted four major sporting events and welcomed almost 700,000 people to the region. From the Vizio® Fiesta Bowl to the NFL Pro Bowl, the Waste Management® Phoenix Open, and Super Bowl XLIX, it was no easy task to coordinate public safety activities across multiple cities for such an extended period of time. More than 100 different organizations and 750 users relied on the U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN) to support situational awareness and coordinate their activities from the early days of planning to the final tee off and touchdown.

Planning & Executing a Game Plan

Planning for these events began more than a year earlier during Super Bowl XLVIII in New Jersey. "I got to see how HSIN helped support situational awareness," said DHS Intelligence and Analysis Southwest Regional Director Anthony Frangipane, "but I also saw more opportunities to use HSIN as a comprehensive planning tool."

When planning efforts intensified last spring, the partnering agencies chose HSIN as their primary information sharing and collaboration tool. Event coordinators assembled a core planning team supported by 24 resource working groups that focused on topics such as law enforcement, logistics, public affairs, intelligence, and, of course, emergency management. They used HSIN to coordinate activities within and among the groups to ensure proper support was provided to each event.

"HSIN streamlined everything so everyone had access to the same materials and resources no matter their location. We preloaded as much information as we could so that it would be readily available when it was needed," said Officer Jim Lawler with the Phoenix Police Department. "As new events were scheduled in the various cities, they were added to a consolidated venue matrix. At any time, HSIN made it possible to easily pull up the date, time, and location of a particular event. We were even able to add details such as estimated attendance so that the individual working groups could see how an event affected their activities and what level of resources would be needed to support it."

Integrating Federal Partners

Due to the scale of the events, broad federal support was provided to state and local agencies to help handle the influx of people and monitor activities. DHS assigned Homeland Security

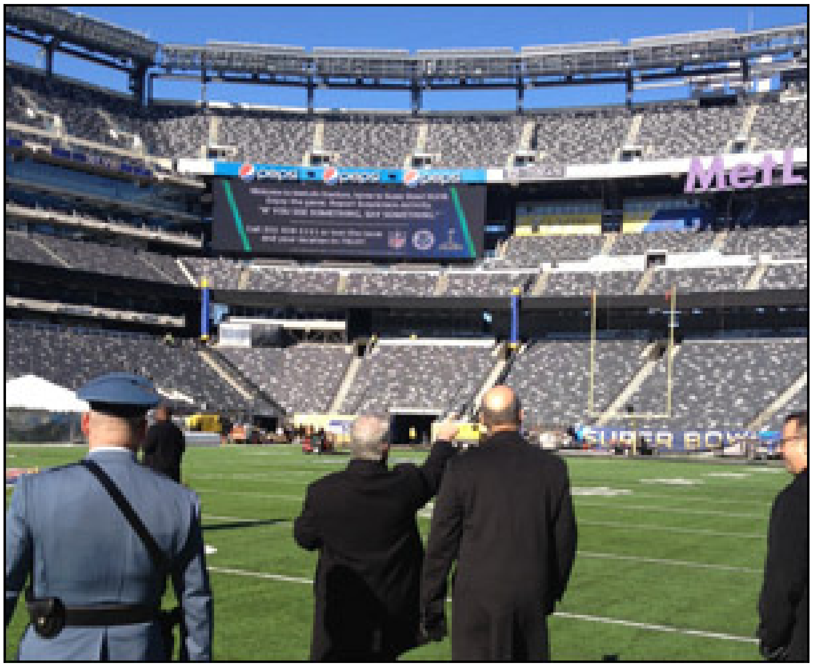
Investigations Special Agent in Charge Matthew Allen as the federal coordinator for the Phoenix events.

"My role was to make sure the local agencies had the tools they needed," said Allen. "Through HSIN, I was able to keep an eye on the entire planning process. When a need was identified, I worked with federal resources so they could provide the necessary support."

If a utility company needed support from the Department of Energy, Allen was there to coordinate. When local explosive ordnance disposal teams recognized a need for additional resources to respond to unattended bags or suspicious packages, he worked with federal agencies in the area to provide assistance. "HSIN was a really great collaboration tool to share information and raise awareness across agencies," explained Allen.

Getting Ready for Kick Off

As the final events drew nearer, five operations centers were set up to monitor activities in real time. Part of the effort included understanding how unrelated incidents could affect the various events.



"I looked at how incident tracking was handled in recent years as part of the Phoenix Open and used their model," said Sgt. Anthony Jones with the Phoenix Police Department's Homeland Defense Bureau and the Arizona Counter Terrorism Information Center. "We tracked everything and posted it on HSIN as part of overall situational awareness efforts so that each sector could evaluate whether any particular incident could impact their activities."

Maintaining Situational Awareness

During the 10 busiest days of event activities, Jones had people in the multiagency coordination center listening to radios and posting the information to HSIN in real time to maintain comprehensive situational awareness.

"During a major event, a lot of energy is spent trying to find out what is happening where," said Jones. "Using HSIN, we were able to capture and post it as it happened so no one had to seek it out."

This information, as well as data pulled from the event planning matrix, was highlighted on a scrolling event tracker in all five operations centers so every agency involved had access to the same information to support decision making in their sectors.

Establishing Positive Public Affairs

Before and during the events in Phoenix, many local and national media outlets reported on the various public safety aspects of supporting so many large-scale, concurrent events. Using HSIN as a virtual joint information center, 150 public information officers from across the region used HSIN to share talking points, press releases, social media postings, and more.

"HSIN acted as a one-stop-shop for us," said Sgt. Trent Crump with the Phoenix Police Department Media Relations office. "We were able to access and share information in a timely fashion and the alerts function made it possible for us to keep abreast of current developments even when we were away from our computers."

> ***"Whether fans were headed to Phoenix for football or golf, public safety officials across the 'Valley' were able to handle the influx of people and coordinate their efforts."***

As media inquiries came in, they were logged, assigned, and tracked in HSIN. As a result, it was easy to see if the same questions were being asked of different agencies and a coordinated response could be provided. "HSIN was one of the most valuable and helpful elements as we put things together for the Super Bowl," said Crump.

Scoring a Win for Everyone

Whether fans were headed to Phoenix for football or golf, public safety officials across the "Valley" were able to handle the influx of people and coordinate their efforts. "In the end, everything went beautifully," said Lt. Jeff Trillo with the Scottsdale Police Department. "With HSIN, we were able to collaborate and provide each event with the attention it deserved. The fans came to town to have a good time and everything went fantastic!"

With Super Bowl XLIX successfully in the books, the HSIN team is already moving forward with support efforts for Super Bowl 50 next year in the San Francisco Bay, California, area! Contact HSIN Outreach with questions or for more information on how HSIN can be used to support local public safety or emergency management operations.

Parts of this article were originally published in The HSIN Advocate, February 2015, and is reprinted with permission.

Janusz Wasiolek is the outreach and mission advocate manager for the U.S. Department of Homeland Security's Homeland Security Information Network. He oversees a team of 18 mission advocates who work with stakeholders to connect organizations across the nation. Previously, he supported the Federal Emergency Management Agency's National Preparedness Assessment Division, developing numerous reports on emergency readiness and preparedness. He is a Certified Emergency Manager, a former paramedic, and holds an M.S. in Engineering Management and Systems Engineering.

InfraGard – Over 400 Sector Chiefs in 84 Chapters

By Sheri Donahue

After receiving credible information about an al-Qaida threat to high-profile buildings where financial institutions were located, the U.S. Department of Homeland Security shared that information through the InfraGard network. InfraGard then used the Sector Chief Program to rapidly disseminate the necessary details to the right people within those institutions.

In the years following 9/11, many efforts have been made to create organizations and improve processes for information sharing related to national security. At the heart of this effort is the protection of the nation's critical infrastructure. Examples show how a threat, attack, or natural disaster – from tornadoes and hurricanes to the threat of a terrorist attack – can have a great and cascading impact on a region.

In an effort to prepare for, respond to, and recover from such events, both Presidential Policy Directive-21 (PPD-21: Critical Infrastructure Security and Resilience) and Executive Order 13636 (EO 13636: Improving Critical Infrastructure Cybersecurity) were issued in February 2013. These documents provide guidance for public and private partnerships to optimize information sharing for the protection of critical infrastructure.

Establishing Sector-Specific Leaders

As the premier public-private partnership for critical infrastructure protection, InfraGard's mission is to provide a conduit for information sharing between and among critical infrastructure owners and operators and government agencies. The Federal Bureau of Investigation (FBI) sponsors the InfraGard program, which has over 37,000 members affiliated with 84 local InfraGard chapters across the country. However, with this many members and chapters nationwide, a system had to be developed to improve the efficiency of that information sharing.

In 2004, the Kentucky (KY) InfraGard Members Alliance (IMA) developed the Sector Chief Program as a means to better know who their members were, what sectors they represented, and what sectors were not well represented. The idea was then to recruit members from those sectors for which there were gaps. Once several members were identified for a sector, one member was selected who would serve as the lead for the sector within the IMA. These select members were the first sector chiefs. The ideal candidates for sector chief were those who had affiliations with other sector-specific professional associations. This would ensure that the sector chiefs kept well apprised of the issues, concerns, events, and best practices of their sectors. They would be knowledgeable as well as have a network for information sharing that extended beyond the membership.

Sector chiefs met periodically with the local board to discuss issues across sectors. They would then assist in sector-specific trainings and information sharing for the quarterly membership meetings. Lastly, sector chiefs would serve as the point of contact for information flow between the members of their respective sectors and government agencies (e.g., FBI, U.S. Department of Homeland Security [DHS], etc.). This could be for more routine purposes (to serve as a subject matter expert for a case) or, in the event of a threat, for the FBI to quickly notify the proper point of contact within the sector in that region.

Sector Chiefs in Action

On Sunday, 1 August 2004, DHS received credible information from InfraGard of a threat to U.S. and international financial institutions based in the United States. Al-Qaida was planning to attack high-profile buildings in which financial institutions were located. Then-DHS Secretary Tom Ridge held an emergency conference call with the state Homeland Security offices (or equivalents) within each state that Sunday afternoon.

Following the call, a representative of the KY Office of Homeland Security contacted the KY IMA leadership and asked for the contact information for the banking and finance sector chief. He then was able to contact the sector chief and brief him on the information that was shared on the call. The sector chief then was able to share information on the threat and the government's evaluation and response with other members of the banking and finance sector. Those members were prepared and ready when their banks and financial institutions opened on Monday morning. There were no surprises and no panic.

Expansion of a Successful Program

In 2004, other IMAs began standing up their own Sector Chief Programs with the assistance of the KY IMA. Some IMAs named a few sector chiefs, whereas others named one for each sector. Their relationships with the state and federal government were different from one to the next as well. In 2013, all 84 InfraGard chapters were asked to form a Sector Chief Program. The InfraGard national leadership and the FBI worked together to develop guidance for the IMAs. The stated mission of the Sector Chief Program is to efficiently "identify sector-specific experts, organize [InfraGard] membership to utilize its resources, and streamline dissemination of information to protect and address vulnerabilities in the critical infrastructure."

Each InfraGard chapter works with the FBI field office with which it is affiliated to determine the priority critical infrastructure sectors for that field office/region. Chapters appoint sector chiefs for one or more of the top sectors. Although some chapters appoint sector chiefs (and deputy sector chiefs) for all sectors, most appoint them only for the priority sectors. One of the benefits for volunteers to serve as sector chiefs is the eligibility for a federal security clearance. However, this will not be processed for all sector chiefs, only those who may require it based on their sectors, locations, expected levels of information needed, and need to know.

An Evolving "National Asset"

As the program continues to grow, more sector chiefs are identified and their roles expanded, InfraGard is planning to identify national sector chiefs that will have affiliations/contacts with their respective sector-specific agencies. These national sector chiefs will be able to connect federal agencies with the sector chief in any area of the country as needed and rapidly share information from a national perspective. As InfraGard has grown and matured over its 19 years, it has evolved to become a "national asset" as quoted in March 2014 by senior leadership in the FBI. The members have become more engaged and active participants in InfraGard and, as a direct result, in the protection of national security.

Sheri Donahue is cyber security and strategic partnerships director for Humana Inc. in Louisville, Kentucky (KY). She previously served as: program manager for security and intelligence at the Indian Head Division of the Naval Surface Warfare Center; director of customer support for DisastersNet Inc.; managing director of the INMA; and executive director and president of the Cyber Conflict Studies Association (CCSA) at the Norwich University Applied Research Institutes. She also served, for 16 years, as an engineer and special programs manager for the Department of the Navy. She has been with InfraGard since 2003, served on the National Board from 2004 to 2012, and has been national president since 2012. As a member of the KY InfraGard chapter in 2003, she co-created the first Sector Chief Program.

Gyrocopters & Other Rapidly Developing Threats

By Rodrigo (Roddy) Moscoso

On 15 April 2015, a 61-year-old mailman from Florida breached restricted airspace over the nation's capital and landed a gyrocopter on the West lawn of the U.S. Capitol building. Although this event did not involve explosives or other hazardous materials, the next incident may not be benign. Communication gaps must be closed.

On 29 April 2015, the House Committee on Oversight and Government Reform held a public hearing concerning the events surrounding the 15 April incident involving Douglas Hughes landing a gyrocopter on the Capitol grounds. During the open session, Committee Chairman Rep. Jason Chaffetz (R-Utah) grilled representatives from the Federal Aviation Administration (FAA), U.S. Capitol Police, Secret Service, and North American Aerospace Defense Command (NORAD) on the apparent failure across the government's airspace security apparatus to either detect or intercept Hughes and his gyrocopter as he travelled from Gettysburg, Pennsylvania, to the West Lawn of the Capitol building.

Technological Capabilities & Inabilities

Previous reports following the closed-door session held for members of Congress a week earlier suggested that NORAD and other agencies had Hughes' gyrocopter "in their sights," but elected not to shoot him down due to fear that doing so might jeopardize public safety. However, at the open hearing on 29 April, agencies testified that this was not the case, and that no weapons were actually drawn on Hughes until the very moment he landed on the Capitol grounds. NORAD Commander Admiral William Gortney acknowledged that NORAD and the FAA currently do not have the ability to distinguish small targets (such as Hughes and his gyrocopter) from a large bird on radar. He added that new technologies currently are being tested that should enable NORAD and the FAA to identify targets as small as a gyrocopter, including even small drones. Gortney offered to provide the committee with additional details on the capabilities of the new system in a future closed-door session.

In the days immediately following Hughes' landing, some pundits and even the media suggested that Hughes did not necessarily pose a significant threat to the Capitol or to other D.C. structures due to the small footprint of the gyrocopter itself. In fact, the USA Today editorial board published an article on 17 April 2015 downplaying the potential damage that a 250-pound gyrocopter could do to any building, noting that, "It would bounce off a structure as robust as the U.S. Capitol or the White House," resulting in minimal damage.

However, during the 29 April hearing, Rep. John Mica (R-NY) noted that Hughes' gyrocopter was capable of carrying 50 or more pounds of cargo. Mica asked Secret Service Director Joseph Clancy what damage 50 pounds of plastic explosive could do to the Capitol building had Hughes chosen a strike on the Capitol building itself. Clancy replied that, "It would be devastating." Mica also noted the failure of the Capitol Police to notify House members and staff via its congressional alert system that Hughes had landed on the West Lawn. In fact, he noted that he and his staff only received notification of the incident, by regular email, from the Capitol Police at 5:02 p.m. adding, "We never heard a thing" until that time, calling it, "another horrible communications failure of the system."

Other Communication Gaps

Beyond the current technical limitations of not being able to monitor a very small aircraft on radar, which kept NORAD, the FAA, and the Secret Service in the dark about Hughes' travels, there were other significant communications failures that negated the possibility for a coordinated response prior to his landing at the Capitol. During the open hearing, Capitol Police Chief Kim Dine stated that a Tampa Bay Times reporter had sent an email to the Capitol Police at 12:59 p.m. (24 minutes before Hughes landed) asking if the Capitol Police were aware that a "local man" was planning to fly a gyrocopter to the Capitol as part of a protest. The email did not specify a time or date of the flight itself. However, the email contained a link to a live Internet feed that Hughes had set up to share his trip with the public.

One minute later, the same reporter called the Capitol Police dispatch center to ask if the Capitol Police had authorized Hughes' flight and landing on the West Lawn. The reporter referred to Hughes by name when he made his second call to the Capitol Police dispatch center. The reporter had first contacted the Secret Service, which referred him to the Capitol Police. At 1:07 p.m., the Tampa Bay Times email was forwarded to a Capitol Police investigative division while, at the same time, a Capitol Police Command Center sergeant attempted to view the feed via the provided link without success. Hughes' live stream had stopped prior to this time, though it had been operational for approximately half of his trip from Gettysburg.

> ***"And it's the unknown threat that we must be instantly ready to respond to. For example, what about someone coming up the Potomac in a small submarine?" asked retired United States Park Police Major David Mulholland.***

Although the Times reporter may not have been explicit about the timing of Hughes' stunt, he nonetheless made multiple attempts to alert both the Capitol Police and the Secret Service over a short period of time, strongly suggesting that the event was imminent. Most significantly, the reporter provided a link to a live feed, which should have indicated to officials that the event was occurring at that very moment.

Connecting the Dots – Before Time Runs Out

At the open hearing, members of Congress seemed incredulous that Hughes' protest flight had been successful given the information provided by the Tampa Bay Times that day. Moreover, Hughes was no stranger to the Secret Service, which had interviewed Hughes in October 2013 after obtaining information that Hughes intended to fly a single-engine aircraft to the Capitol. Clancy noted that, following this interview, the Secret Service determined that Hughes did not pose a threat to areas under its protection, but the agency nonetheless had shared information about Hughes with other law enforcement agencies following the 2013 interview. This led to questions from members on how Hughes, having been previously known to the Secret Service, could have been such a surprise when the Tampa Bay Times provided his name to them more then 20 minutes before he landed.

Chaffetz asked the panel, “Do you all not monitor social media? Is Twitter a new thing for ya? This stuff is out there. Try Google alerts.” These comments and questions underscore how near real-time communication channels such as Twitter and Facebook, coupled with robust data sharing and information access, could be leveraged during rapidly developing events. Theoretically, when the Capitol Police were provided with Hughes’ name at 1:00 p.m. by the reporter, agency personnel would have searched and found a record of the October 2013 interview, connected the dots, put two and two together, and realized that Hughes was indeed attempting to fly and land at the Capitol at that time.

In this scenario, the Capitol Police would have alerted its partner agencies, including the FAA and NORAD, which may have had time to intercept Hughes in flight – Hughes himself expected that this was a likely possibility. However, this scenario is dependent on human resources being able to quickly coordinate and collaborate with partner agencies around a common set of data. Although great strides have been made in connecting various command and watch centers across agencies and disciplines since the terrorist attacks of 9/11, including the creation of the FAA’s Domestic Events Network (DEN), which shares information with more than 130 agencies in real time, Hughes’ success demonstrates that technology is not a panacea.

Had agents with the Secret Service, NORAD, FAA, Capitol Police, and United States Park Police all been in the same room together when the first email and call came in, the above scenario may have played out differently, with Hughes and his gyrocopter ending up in the Potomac River along with his letters. Of course, the next time it may not be letters. More importantly, no such room exists that contains the range of agencies and skills currently charged with monitoring and responding to threats to the nation's capital. But maybe it should.

What to Do – An Insider's Perspective

Retired United States Park Police Major David Mulholland believes that the best way to deal with a rapidly developing threat is to ensure that "the right people are in the same room together," according to a personal interview on 23 April 2015. In his 20+ years managing and supporting events in and around the National Mall in Washington, D.C., Mulholland stood up dozens of joint operations centers, which included representatives from local, state, and federal agencies, and represented a wide range of disciplines, which included traditional law enforcement, transportation, fire, emergency medical services, building management, and meteorology. "They must be in the same room together, and with access to their agency's information and datasets, as well as to their own people and resources. This allows everyone to collaborate in real-time and to share their perspectives and, when necessary, engage their people in a truly collaborative fashion across the group," Mulholland said.

He noted that establishing and maintaining a joint operations center like this 24/7 is logistically difficult and expensive, but that it also is the best way to leverage the talent and resources of the myriad agencies already charged with an operational role in protecting the nation's capital. "Nobody was thinking and planning for how to handle someone flying a gyrocopter to the Capitol, but you better believe that they are now," Mulholland said. "And it's the unknown threat that we must be instantly ready to respond to. For example, what about someone coming up the Potomac in a small submarine? It could be an entirely new threat, and we'll need every agency participating instantly on coordinating the best response. And you can only do that by being together in a physical space designed just for that purpose – it won't happen via telcon [telephone conversation] or video call," Mulholland continued.

Technology provides real-time access to information in nearly every conceivable way, even on new smartwatches. However, the alert one receives is only as accurate (and timely) as the people who are sending it. Hughes' gyrocopter incident has provided the response community with an opportunity to consider how this event could have been handled differently, by whom, and from what location. If the group that testified on 29 April discusses these questions around the same table, they may find that keeping the dialogue going, in the same location, could be a good start.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

Defining & Working With 21st Century Mass Media

By Anthony S. Mangeri

Mass media can be allies or adversaries to emergency management agencies. The key for these agencies is to ensure that media outlets are sharing accurate public safety and incident-related information from trusted and reliable sources. This means that emergency managers must understand news media objectives and develop mutually beneficial working relationships.

The ability of emergency management to communicate strategies and inform the public adequately during times of crisis is essential. Equally important is the value of the mass media as a partner in providing guidance on preparedness, creating risk reduction strategies, and securing the reputation of an emergency management organization. Media outlets have evolved into a 24-7 activity. Today's popular media sources are distribution systems designed to collect information to convert into content. The content then is prepared to draw an audience. In addition, the audience make-up is essential to draw advertising; and advertising drives revenue.

Defining Mass Media

The concept of "media" has changed significantly over the years. Mass media may be defined as a mechanism to distribute information to a large part of the population. Today's mass media includes traditional systems such as television, radio, newspapers, magazines, and the like.

The addition of the Internet has created distribution systems that include subscription e-mail lists, blogs, and social media. All of these sources of news have the ability to manipulate the community's perception of, attitude toward, and sense of what is and is not important.

With direct access to mass media outlets and social media sites via mobile Internet, it appears that anyone with a smartphone is, in fact, a potential reporter, as well as a potential consumer. Many times, information is being posted to social media and Wikis as incidents unfold. According to the Pew Research Center, in 2012, approximately 50 percent of the public retrieve their news from online sources. This percentage is higher than those who rely on radio and newspapers. With 71 percent of those between 18 to 29 years olds getting their news online, the trend will continue to increase.

Making News in Modern Society

Conventional wisdom says that people view media and create their own meanings from what they see and read. Today's news consumers play an active role in the story.

News stories are written to a basic formula. Like good fiction, most news stories have a victim, a rescuer, and a villain. News stories have common elements to consider when creating the storyline. A good emergency manager or public information officer needs to keep the storyline in mind when working with the media.

Editors look for certain characteristics when reviewing potential stories. To be newsworthy, it may be desirable to have conflict or controversy among the story's actors. Stories involving disasters, accidents, acts of heroism, and any story involving children and/or celebrities tend to be attractive to mass media editors. Events that are quirky, unusual, or involve animals or human interest also may have higher priority.

Using the Media as a Force Multiplier

One of the best ways for emergency managers to work with the media – as with the community as a whole – is to develop relationships and build trust and credibility with media outlets before an incident or disaster. It is important to educate both the community and the media about disasters and the steps needed to mitigate potential threats.

Reporters are not friends nor enemies, but rather gatherers of information and content for storylines. This is critical to understand when working with reporters. A good incident commander and public information officer know what information is needed to motivate an effective and appropriate community action, which can be more effective when shared through mass media outlets.

In a crisis or incident involving a portion of the community, the public's need for information is tied to a sense of safety and security. Limited access to information may create heightened public emotions and assumptions about the incident and threat to safety. The emergency management agency's need is to provide credible and accurate information as quickly as possible. The benchmarks of a solid public information effort include news reports that are: accurate, informative, timely, open, and empathetic.

Reporters need to be professional and fair in their reporting. And, emergency managers and public information officers should not allow disagreements to dissolve into broadcasted arguments that no one can win. Responses to questions should never be casual or cavalier. Moreover, it is important for agency representatives to follow through in a timely manner when they tell reporters that they will get back to them with the information they need.

Anthony S. Mangeri, MPA, CPM, CEM, is the director of strategic relations for fire services and emergency management and is on the faculty of the American Public University System's School of Security and Global Studies. He has more than 30 years of experience in emergency management and public safety. He also has spent much of his career integrating public health and community emergency management systems. During the terrorist attacks of 11 September 2001, he served as operations chief at the New Jersey Emergency Operations Center, coordinating that state's response to the passenger-aircraft crashes into the World Trade Center.

Bridging the Public-Private Sector Divide

By Catherine Feinman

At the April 2015 Ready Chesapeake meeting, members of this nonprofit group discussed ways to build business continuity within Annapolis-area communities and created a survey to reach out to other jurisdictions for suggestions. Practitioners (149 public sector, 80 private sector) from 47 U.S. states, Washington, D.C., Canada, and Martinique shared their insights from both the public and private sector perspectives.

Business continuity is important not only for the businesses themselves, but also for the public sector agencies that depend on private sector resources, such as critical infrastructure to maintain continuity of government. As such, there is significant value in bridging the current information gaps that exist between the two sectors. Although public and private sector responders are in agreement on the top answer to each of the survey questions, a closer look reveals some significant discrepancies in the value placed on certain resources.

Resources for Obtaining Business Continuity Information

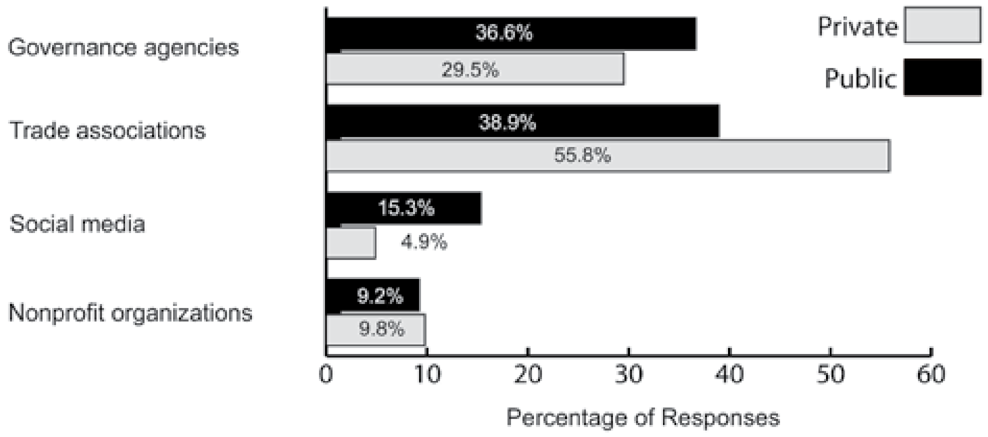
As shown in Figure 1, the majority of private sector respondents believe that trade associations are the best resource for obtaining business continuity information, with governance agencies as the second highest response at just over one-quarter. Public sector respondents, though, were almost equally divided between these two categories.

This shows that perhaps there is a gap between the value public sector agencies place on their resources and how the target audience (the private sector) perceives these resources. Another interesting observation is the difference in value placed on social media for business continuity information. If the private sector depends on trade associations and governance agencies for critical information, then that is where the public sector focus in distributing such information also should be.

Of course, there is no single solution to such complex issues, and a combination of all of the above is necessary, with some being more effective than others at certain times and under certain circumstances. In any case, though, there needs to be a collaborative continuity effort between the public and private sectors. Some suggestions from respondents for sharing continuity information include:

- Annual conferences for both private and public sectors
- Direct engagement with businesses
- Emergency management/preparedness partnerships
- Federal Emergency Management Agency resources

Figure 1
Which resource is the best way to obtain business continuity information?



- InfraGard
- Local Emergency Planning Committees
- Local and state government-business informational meetings
- Outreach through media
- Private sector solution providers
- Related business associations
- Standards organizations – for example, International Organization for Standardization (ISO)
- Webinars
- Workshops for businesses

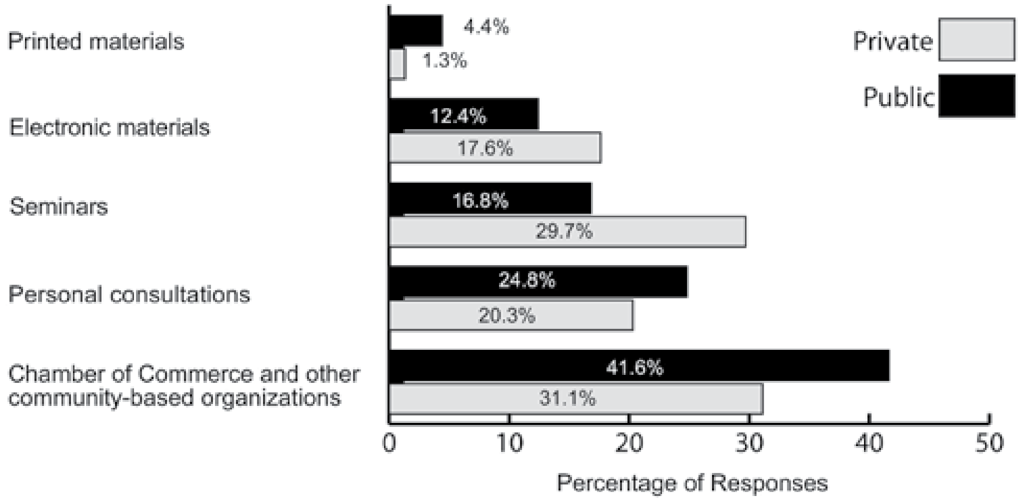
Each private sector company or organization is different, with different combinations and levels of risks and vulnerabilities, which require continuity of operations documents specific to their needs and requirements. However, direct contact between sectors would go a long way in bridging the information gap and improving business (and government) continuity. One public sector respondent suggested the “use of authorizing federal international agreements as leverage for the private sector to share their successful security methodologies with the federal government.” By sharing best practices and lessons learned among the jurisdictions and sectors, the benefits of collaboration and their resulting fiscal efficiencies and effectiveness can become more apparent.

Engaging Small Business in Continuity Planning

Small businesses are valuable assets that cannot be forgotten within communities. In the second question, survey participants were asked about the best way to engage small business in continuity planning (Figure 2). Again, the public and private sector respondents agreed on the top answer as the Chamber of Commerce and other community-based organizations and the bottom answers as printed and electronic material, but disagreed on other ways to engage the private sector. Private sector respondents reported almost equal weight between community-based organizations and seminars. A much lower percentage on seminars for public sector respondents shows that perhaps it would be beneficial to invest more public sector resources into seminars.

Once again, there is no single silver bullet to reach the small business community. A combination of these and other avenues may be needed to reach the diverse private sector target audience, which may not have knowledge of or access to the full range of resources available. Through direct contact and interaction within the business community, the public sector can help build a stronger culture of preparedness.

Figure 2
How is the best way to engage small business in continuity planning?

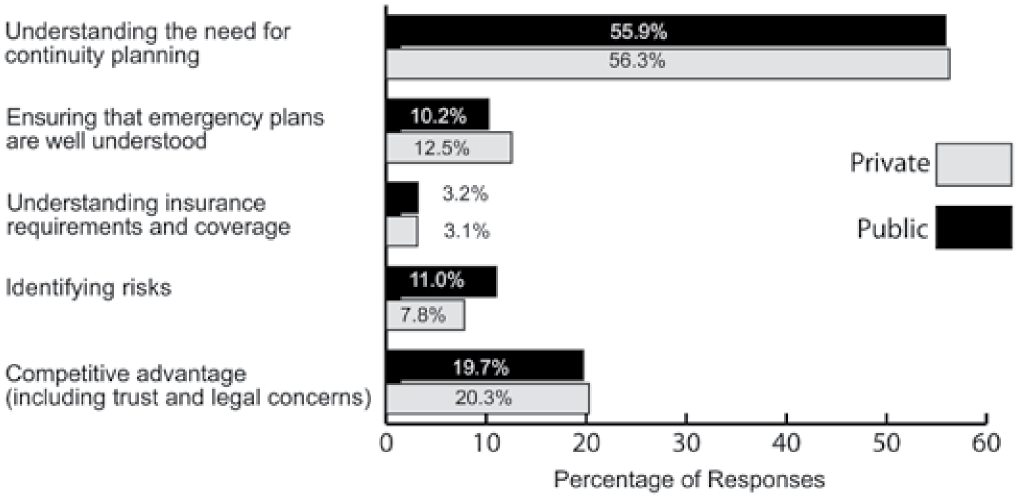


Gaps in and/or Barriers to Continuity Planning

Responses from the public and private sector respondents were in agreement with regard to identifying the greatest gaps in and/or barrier to continuity planning for the private sector. The bottom line is that the need for continuity planning is not well understood (Figure 3). Competitive advantage (including trust and legal concerns), emergency plans, risk identification, and insurance requirements and coverage are all topics that must be addressed within the public-private sector communication efforts.

Time, costs – both real and perceived – and complacency were listed by both sectors as barriers to continuity planning. Resource allocation can be particularly challenging in small businesses with few personnel available to create, implement, and regularly update a business continuity plan in addition to the daily responsibilities required to maintain profitability – thus, business continuity in nonemergency operations. In the public sector, having the personnel and time to reach out to the large business community may be difficult. Even the businesses that are aware of the importance may "not place disaster preparedness high on their 'to do list'," as stated by one public sector respondent.

Figure 3
In your experience, what is the greatest gap in and/or barrier to continuity planning for the private sector?



Cost is another big concern for businesses. Planning, implementation, training, and insurance are some of the costs associated with business continuity. The long-term benefits for costs – such as hardening assets against cyberintrusion – in the short-term may be difficult to foresee or to explain to stockholders. One public sector respondent suggested that, "To be successful, you must have short-term benefits [e.g., insurance rate drop]. If short-term benefits do not exist, a company will continue to be penny wise and pound stupid." To justify costs beyond insurance, a cost-risk analysis would be helpful.

Complacency is another gap expressed by respondents from both sectors. "It won't happen to me." Or, "The other guy is not doing it, so why should I when I need the resources somewhere else?" Businesses need to be incentivized to invest resources into preparedness. "Many businesses don't understand some of the basic risks and costs. If they understand the basic risks and costs, some basic support such as planning seminars and best practices can provide significant value," stated one private sector respondent.

However, perhaps an even bigger incentive came from a respondent in the public sector, who stated that, "The private sector does not understand how ill prepared the public sector is. Or how they need to collaborate before an event." The public and private sectors need to find common ground in terminology, trust, and communication to ensure overall community resilience. To address the complexities and contingencies related to a disaster, it is important to change the "government interference" mindset into a "government partner" relationship by "identifying and communicating how [continuity of operations] and preparedness (resiliency initiatives writ large) can be used to bolster normal operations and ultimately provide a competitive advantage."

Overcoming Public-Private Sector Barriers

As one respondent stated, "A few dramatic real-life examples provide more incentives than all the professional [public relations] material available." Respondents shared methods they have used to overcome some of these barriers. Face-to-face meetings, seminars, and joint trainings have proven to be successful for some public and private sector respondents, whereas others still see many existing barriers. Public sector respondents who have found success did so by:

- Identifying small business champions;
- Sponsoring training seminars and inviting local resources to participate in planning and emergency response training;
- Providing supportive information and messages from top leaders;
- Working with individual businesses to develop their own plans;
- Creating a private sector portion for the operational area emergency operations center;
- Having a government business liaison;
- Identifying the gatekeepers in the community and getting them involved in the planning process;
- Understanding the needs of the community from the community instead of assuming what the needs are;
- Working with InfraGard as well as holding regional meetings in the state with emergency management and homeland security partners;
- Gaining executive buy in while working with risk safety and emergency management professionals;
- Making preset agreements with companies needed for operations such as mass fatality, hotels for families, refrigerated trucks, etc.;
- Using examples of local businesses that have suffered a catastrophic loss without a plan;

- Working with organizations to understand how they fit into the continuity of operations plan and how they fit into the entire Continuity of Operations/Continuity of Government concept; and
- Engaging and recruiting businesses through the Chambers of Commerce to work on continuity planning and disaster risk reduction projects.

Private sector respondents have found success by:

- Participating in Homeland Security Exercise and Evaluation Program (HSEEP) and national-level exercises to identify flaws in existing plans;
- Attending and making personal contacts at business continuity seminars and meetings hosted by the Fire Department, Office of Emergency Management, Local Emergency Planning Committee, Association of Contingency Planners, or local Chambers of Commerce;
- Offering training to key government officials and leaders;
- Reaching out to county emergency responders and engaging them in training to help support onsite teams;
- Meeting with offices for personal consultations and explaining insurance and regulatory requirements, as well as identifying risks and competitive advantage;
- Embracing the need for a continuity plan, placing vital continuity documents in the hands of key personnel, on web-based-sites, and in paper form in Standard Operating Procedure manuals at several sites;
- Understanding the requirements, developing the skills to implement the requirements, and maintaining the program;
- Designating a staff person to build the plan and hold everyone else accountable, which took the decision out of management’s hands and created an environment where everyone understood they would be affected;
- Teaching emergency management to private sector companies;
- Communicating the financial/economic value of preparedness efforts through modeling and simulation tools using actual numbers from business owners;
- Including all employees in identifying potential risks, researching other community and area risks, and searching for potential solutions;
- Creating a culture of preparedness and hiring smart and experienced people;
- Developing public-private partnerships through emergency management associations; and
- Realizing the return on investment.

In some cases, public sector respondents expressed frustration with making many outreach efforts, but with little return. "We have not overcome the barrier but we continue to educate small business owners and those organizations that work with small businesses. It may take them 4 or 5 times of hearing the importance before taking even one small step to creating a plan." However, another public sector respondent offers the following encouragement, "Just keep putting the word out (over and over again, for years) and offering freely available tools and tips. Those who understand the cost benefit will come around eventually."

Regulations & Laws That Encourage Business Continuity

Depending on the infrastructure and industry involved – as well as local codes, laws, and regulations – the amount of regulations and continuity planning guidance may vary.

Although current laws do not require many private sector businesses to have continuity plans, there are laws, codes, regulations, and programs in place to help promote more resilient private sector operations. These include, but are not limited to:

- Business Continuity Management Systems: Requirements with Guidance for Use (ANSI/ASIS/BSI BCM.1-2010)
- Consumer Credit Protection Act
- Disaster Resiliency and National Fire Protection Association (NFPA) codes and standards, more specifically NFPA 1600
- Federal Communications Commission (FCC) guidelines
- Federal Continuity Directive 1 (FCD 1)
- Federal Continuity Directive 2 (FCD 2)
- Federal Preparedness Circular 65
- FEMA's Business Continuity Plan
- Foreign Corrupt Practices Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Hospital Preparedness Program (HPP)
- IRS Procedure 86-19
- Occupational Safety and Health Standards Laws and Regulations
- Presidential directives including:
    - Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
    - Presidential Policy Directive 8 (PPD-8): National Preparedness
- Project 2014-04 Physical Security (CIP 014)

- Public Health Emergency Preparedness (PHEP) cooperative agreements
- Sarbanes-Oxley Act of 2002
- Service Organization Control (SOC) Reports
- Superfund Amendments and Reauthorization Act (SARA) of 1986
- Telecommunications Act of 1996
- The Joint Commission Standards
- The Voluntary Private Sector Preparedness Program – PS-Prep™ and Small Business Preparedness
- U.S. Food and Drug Administration's Food Safety Modernization Act (FSMA)
- U.S. Securities and Exchange Commission (SEC) laws

With so much at stake, whether they like it or not, the public and private sectors are dependent on each other for building resilient communities. Respondents from both the public and private sector offered the following suggestions for encouraging private sector businesses to develop viable and sustainable continuity plans:

- Ask vendors and suppliers to provide their business continuity plans when they make bids for contracts.
- Develop contractual relationships to build supply chain security.
- "Require continuity of operations planning to be completed as a condition of full insurance coverage and benefits. Less planning results in reduced benefits. More planning results in better benefits and reduced rates."
- Understand that, although "some laws and regulations are necessary, they do not correct problems. They merely guide private activities in preferred directions. Finding real solutions requires a much better understanding of human nature."

True business continuity and resilience efforts require more than a simple "check the box" process. It requires collaborative, long-term public-private relationships and communication. Community resilience takes a whole community approach. When disaster strikes, some businesses may not recover. A well-planned business continuity plan, coupled with established public-private relationships, offers an added level of insurance. After all, "No law says you have to stay in business."

Catherine Feinman joined Team DomPrep in January 2010. As the editor, she works with writers and other contributors to build and create new content. With more than 25 years experience in publishing, she previously served as journal production manager for Bellwether Publishing Ltd. She also volunteers as an emergency medical technician, firefighter, secretary of the Citizen Corps Council of Anne Arundel County and City of Annapolis, and a Community Emergency Response Team (CERT) trainer.

FilmArray