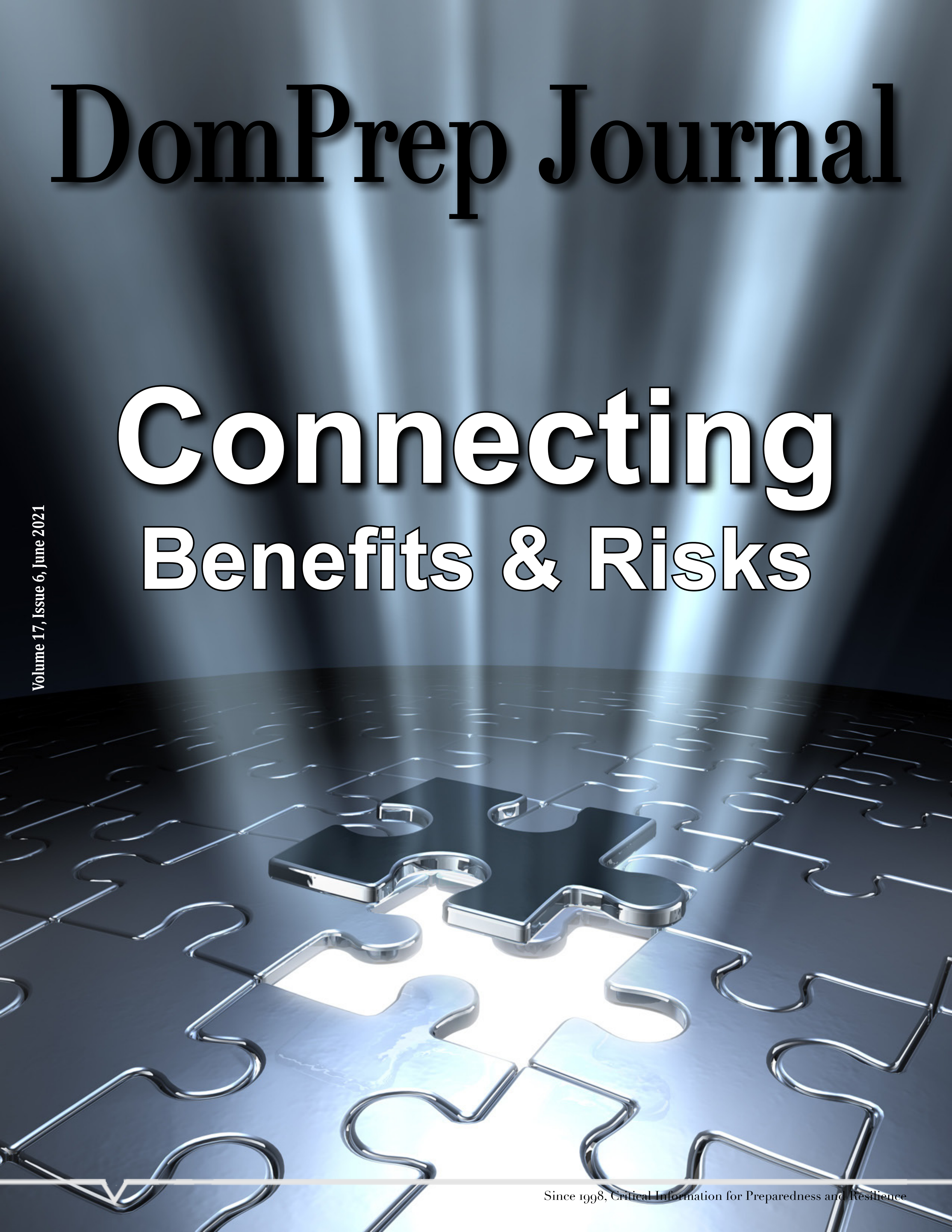
DomPrep Journal



Connecting

Benefits & Risks

Volume 17, Issue 6, June 2021

Since 1998, Critical Information for Preparedness and Resilience

TELEDYNE FLIR
Everywhereyoulook™
WE'VE GOT YOUR BACK. LITERALLY.
POLICE

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

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

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

Carole Parker
Manager, Integrated Media
cparker@domprep.com

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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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

Pictured on the Cover: ©iStock.com/jgroup

Dräger

MADE IN
★ USA ★
SINCE SEPTEMBER 8, 2020

With a new plant in the USA, Dräger has you covered

For ground personnel working in dusty environments, respiratory protection is essential. The Dräger X-plore® 1750 N95, our next-generation particulate filtering facepiece respirator, offers distinct improvements in comfort and protection. And it's now made right here in the US.

FOR MORE INFORMATION VISIT WWW.DRAEGER.COM

Dräger. Technology for Life®

Connecting: Benefits & Risks

By Catherine L. Feinman

To take a multidisciplinary, multijurisdictional approach to disaster preparedness and response, agencies and organizations must connect both in person and virtually. Mutual aid agreements enable agencies to share resources and develop a collaborative strategy for addressing emerging threats. Although predicted by experts, the threats that presented over the past year – namely, a global pandemic and large-scale cyberattacks on critical infrastructure – still caught many communities by surprise.

As many people who were still able to work were forced to suddenly do so from home, the social and connectivity challenges were quickly realized. Virtual platforms experienced glitches and overloads, technologies at home were insufficient or absent, and the lack of in-person gatherings have had long-term consequences that are still yet to be fully understood. Professional and personal lives melded, yet goals and objectives still needed to be met.

This edition of the *DomPrep Journal* is about connecting, which is a critical part of work and society, yet it is not without risk. Public-private partnerships and agreements can bring together valuable resources such as command trucks that can be repurposed to support volunteer efforts that supplement government operations. These connections also ensure that these critical resources are ready and available with trained personnel when needed during a disaster.

Similarly, the healthcare supply chain requires routine collaboration by both public and private entities during non-emergencies to safeguard continuous operations when the supply chain demand is overwhelming. By connecting manufacturer supply with end user demand, government agencies can help make sure supplies continue when they are needed the most.

The past year has provided many workplace lessons learned to help prevent future broken connections from causing resource shortages and communication delays. However, the dependence in online technologies and critical infrastructure resources has caused bad actors to intervene and access operations of both virtual and physical assets.

The growing online presence for building work, school, and personal connections has also had its downsides. The dependence on virtual interaction has increased the risk to vulnerable populations, especially children. The virtual platform provides more opportunities for child predators and human traffickers. As such, it is critical that all community stakeholders communicate and work together to rebuild lost connections and create new ones that benefit the whole community.

The Other Life of Command Trucks

By Erik Westgard

For many years, large outdoor sporting events have requested government and nongovernment organization mobile command and communications trucks to support races. Although traditionally used by incident commanders, volunteer amateur radio groups have found various ways to collaborate during special events and use these resources in Minneapolis, Minnesota to support medical operations.

Mobile command and communications vehicles are used in a variety of radio-related roles. In Minneapolis, public-private agreements between law enforcement agencies and ham radio operators have proven to be mutually beneficial for special event planning and emergency response. Command trucks provide valuable resources that enable radio operators to provide more robust response communications during large and small events.

Communication Links at Large Events

Incident commanders for the Medtronic Twin Cities Marathon weekend have been St. Paul Fire deputy emergency medical services (EMS) chiefs, who would rather be staged at the finish line. In that location, medical professionals are better positioned to gauge the health status of individuals by observing the faces and condition of runners as they complete the race. With over 10,000 athletes on the racecourse and the possibility of temperatures approaching the danger zone for heatstroke, it is critical for EMS to stay ahead of an impending possible mass casualty incident.

Source: Erik Westgard

Using detailed documentation – medical plan (ICS Form 206), incident action plans, and various internal documents – the medical system is able to respond without delay. By long-standing agreement, a 911 call is made for a runner down. In this way, a rolling emergency room is on the way and prepared for life-threatening scenarios such as a heart attack.

At the same time, the volunteer medical team takes immediate action. Amateur radio operators, stationed at regular intervals, call in the bib number and location of the injured runner. An assigned incident dispatcher in one of four net control stations or command trucks correlates the 911 report and radio reports. If they match, a "thumbs up" is exchanged with EMS medical command. In this way, errors are addressed and duplicate dispatches to the same scene are prevented. For example, in 2019, a dispatch call went out from a unit on an unmonitored government radio channel. This was heard by an EMS employee volunteering that day who recognized that there was no matching 911 call. The EMS volunteer initiated a dispatch, so the error was caught.

Command trucks should not sit and collect dust when they can do so much more to enhance local response efforts and public-private event communications.

Volunteer medical providers at aid stations, on the racecourse (i.e., bike medics), and in a 40x80 foot main medical tent care for minor conditions that, in their judgement, can be treated locally. These stations relieve strain on the 911 system and area hospitals.

Serving as an intertie between amateur, event and government radio channels is one role for the command trucks. In the annual medical communications plan for the Medtronic Twin Cities Marathon, there are four amateur radio repeaters and two event-rented radio medical channels (with 350 rented UHF radios). In the case of larger events, the communications mix can include up to 10 rented radio channels as well as many public safety radio talk groups. This is all documented on the ICS Form 205 and on the incident action plan.

Coordination Roles at Smaller Events

Command trucks also have a role at smaller events. For example, Minneapolis hosts a summer race – the Red, White & Boom half marathon – that welcomes a few thousand runners and has around five aid stations. In this case, the Hennepin County Sherriff Incident Communications Center (ICC) truck arrives with a team of special deputies. These volunteers staff the aid stations with communicators and park the truck near the finish line. Government radio systems are used by the authorized volunteers. Race-rented radios are used via a temporary antenna in the truck to talk to the race medical director and aid station volunteer staff.

The incident commander for this event is a Hennepin Healthcare EMS supervisor. On a normal day, the event and volunteers run the show. If a mass casualty incident is declared, there is literally a chair in the command truck for the incident commander to occupy. Until then, he/she also prefers to be on the finish line next the medical director, as it is often a hot day. In 2019, volunteer special deputies were given authority to coordinate dispatches under the supervision of the incident commander. This model is used for parades and similar events all summer.

Source: Erik Westgard

In another case, the mobile command and communications truck has been outfitted with inexpensive mesh/Wi-Fi radio gear and IP video cameras. With open-source broadcast software, trucks and portable cameras can be used to capture video and stream it, as required, to an emergency operations center or even to social media sites. The remote cameras and multiple vehicles were used with the mesh network to cover a 40-mile dogsled racecourse on a 20,000-acre lake for the 2020 Klondike Dog Derby.

Every June, The National Association for Amateur Radio hosts ARRL Field Day. It is common to run that 24-hour contest/event from command trucks and emergency operations centers as a preparedness exercise.

Planning for Future Events

Recommendations regarding command trucks and volunteers:

- To justify their existence, trucks need to be used. If trucks are too closely secured, they will collect dust and may be vulnerable to disposal or scrapping. This has happened in the Minneapolis area. Several surplus command trucks listed recently online had surprisingly low mileage.

- Repeated use and training are critical. Underutilized gear will be unfamiliar to personnel if needed in events or emergencies.
- Oversight is needed to stay current. Equipment and software suites (e.g., analog video) will become outdated.
- Trucks provide resources that can be shared with volunteer responders: extra open antenna mounts, cable ports, rack space, electric outlets, and powerful Wi-Fi are always helpful.
- Ham radio and other volunteer equipment can be installed on trucks. However, for security reasons, it may be better to air gap from government networks. Do not share routers or switches from gear that is not enforcing the same security policy. Best practice is to not have secure network segments at all, with every user and usage being authenticated "zero trust."
- Deploying trucks at events provides visibility and builds rapport between response agencies and parade goers, runners, skiers, and other community members.
- Regular live testing of trucks and equipment is a viable solution for many public safety communications problems. Capacity building with other agencies and nongovernment origanizations can enhance the ability to scale.
- The recent practice of removing or not ordering tall antenna masts from command trucks seems ill advised when deploying to rural or storm-damaged areas.

Many local and state agencies have valuable resources that are underutilized. Command trucks are one example of equipment that can be repurposed and shared with volunteer organizations that assist in special event planning and response. Such collaborative efforts not only provide resources that may otherwise be unavailable to volunteer organizations, they also enhance agencies' ability to maintain equipment during normal operations and enhance response efforts for special events. If command trucks and other emergency equipment are collecting dust, there is a good chance they will not be ready and usable when disaster strikes.

Erik Westgard, MBA, NY9D teaches digital strategy in the College of Management at Metropolitan State University in Minneapolis. He coordinates ham radio volunteers for the Medtronic Twin Cities Marathon, Red, White & Boom Half Marathon, and the Loppet City of Lakes Winter Festival. His most recent project is the conversion of a dozen surplus construction light tower trailers into mesh networking tower generator units to support events and Minnesota VOAD.

Online & Social Media Risks – Protecting Children, Part 1

By Michael Breslin & Robert Lowery Jr.

The COVID-19 pandemic brought child predators into people's homes. In the critical areas of human trafficking and child exploitation, the risks to children increased due to criminals shifting their methods and techniques to online streaming services. Increased virtual learning and stay-home mandates forced children to transition from a classroom environment to home learning via virtual platforms. This transition done in the perceived safety of a child's home under the supervision of his/her parent was and remains fraught with inherent danger.

The Federal Bureau of Investigation (FBI) recently warned that there is an increased online presence of children, and offenders are taking advantage by directly communicating with many of them. Offenders are using various internet chat rooms, online gaming platforms, and social media applications – bringing themselves right into living rooms and children's bedrooms. This obviously creates a heightened risk of sexual exploitation, coercion through sextortion, and even sexual victimization when lured from the safety of their homes. According to the FBI press release:

> *Online sexual exploitation comes in many forms. Individuals may coerce victims into providing sexually explicit images or videos of themselves, often in compliance with offenders' threats to post the images publicly or send the images to victims' friends and family.*

"Pedophiles are disrupting Zoom sessions. The FBI wants your help in finding them" read the 27 May 2020 NBC news story citing a report by the FBI that "more than 240 people disrupted Zoom sessions by broadcasting videos depicting child sexual abuse." This adaption of criminal and depraved individuals only increases the need for proactive cyber awareness and physical security measures for the digital devices children access.

The Internet Threat Landscape – Social Media

This ever-interconnected world relies on the dependability and convenience of technology. Over the past decade, criminals have become increasingly adept in using open-source (i.e., publicly accessible) information to gain access to sensitive systems in both the public and private sectors. It is exceptionally easier for criminals to obtain what they need from the information published on open-source social media platforms.

The detailed data posted on social media can unwittingly offer a front row view into daily lives, habits, and whereabouts. Social media platforms contain target-rich data such as geospatial information, online photos, and personal identifiable information (e.g., name, age, date of birth). All this information can assist those who are committed to perpetrating acts of child exploitation. The ease of use, availability, and anonymity the internet offers makes it the conduit of choice for criminals. According to a 2021 Pew Research Center survey, 41% of Americans have experienced some type of online harassment.

Daunting Challenge

It is an unfortunate reality that missing and exploited children continue to be a massive challenge globally. According to the National Center for Missing & Exploited Children (NCMEC), more than 21.7 million reports of suspected online child sexual exploitation were made to their CyberTipline in 2020. One form of exploitation reported to the CyberTipline is child sex trafficking. Of the more than 26,500 endangered runaways reported to NCMEC in 2020, one in six were likely victims of child sex trafficking. Today, 15 is the average age of child sex trafficking victims reported missing to NCMEC.

> ***Online luring has reached a level that it should be part of law enforcement's risk assessment process when reasons for the disappearance is not clear.***

According to the FBI, there were more than 421,000 National Crime Information Center (NCIC) entries for missing children in 2019. Although parents and caregivers must recognize their role as the *first line of defense* when it comes to protecting children, it is critical for everyone to identify the signs and know how to intervene appropriately and effectively. Warning signs of those victimized by sexual exploitation may include:

- Emotional, angry, and aggressive outbursts
- Changes in behavior – such as, becoming introverted or withdrawn, perhaps isolating themselves from everyone else in the home
- Attempts to conceal or hide online activity
- Having social media accounts that parents do not know about
- Spending excessive amounts of time online
- Threatening to run away from home
- Suspicion of drug or alcohol abuse
- Lacking concerns for themselves; engaging in self-harming behaviors, including cutting and other high-risk activities

Luring of Children by Offenders vs. Runaway Children

Various social media applications and internet chatrooms offer unrestricted access to children. The motivation of the offenders may vary, but the most common is sexual – either through victimization (direct contact), exploitation (child sex trafficking or sharing sexual images or videos), and sometimes extortion of money.

Offenders generally either disguise their identities or present themselves as someone typically non-threatening or legitimate to the child, like taking on the persona of a child of similar age and gender. In the case of a female child, they may present themselves as a similar age male suggesting that they may have interest in them as a girlfriend. Others may suggest opportunities for the children to work as paid models or escorts with promises of earning a lucrative income and creating a path to a better and glamourous life.

In many cases, the initial goal is to lead or coerce the child into an inappropriate conversation of a sexual nature – something he or she may not normally engage in. Depending on the circumstances, this commences the grooming process that may go on for hours, days, weeks, or even months. Once the child participates in the conversation and it reaches a certain level, the offender then threatens to reveal the content to their friends and families or post the information on the internet for others to see. This then becomes a form of blackmail, where the offender then demands additional sexual content – usually sexually explicit photographs (nudity, etc.) or video (recorded or live) of a sexual performance. This common criminal practice led to the term "sextortion," which is NCMEC defines as:

> *a new online exploitation crime directed towards children in which non-physical forms of coercion are used, such as blackmail, to acquire sexual content from the child, engage in sex with the child, or obtain money from the child.*

In some egregious cases, offenders attempt to make direct physical contact with the child. They either arrange to meet them or demand that the child leave their home. Offenders travel, sometimes great distances, to either a pre-agreed upon location or even meet them right outside of their homes. In past cases, witnesses reported seeing the child jump out of their bedroom window and run directly to the awaiting car. Once contact is made, the offender takes the child to a location where the physical sexual victimization occurs. The child either returns home or remains with the offender for an extended period for additional victimization.

In some cases, the duration the child was away may have been relatively short. Therefore, parents or caregivers may not even be aware the child had left or was missing for any period of time. In these cases, the child may not report the victimization – largely out of fear.

However, when the child is discovered missing, the incident may initially present itself to law enforcement as a runaway. Obviously, this conclusion is based on the appearance of the child voluntarily leaving home and the lack of knowledge about the online grooming activity by the offender and the sextortion. Regardless, once this has been discovered, the missing incident should no longer be treated as a runaway. Instead, they should be considered as high-risk cases of "child abduction, facilitated by technology," which calls for an escalated response and search.

The rate and prevalence of online luring has reached a level that consideration of the possibility of luring should be part of law enforcement's risk assessment process when taking a report or investigating any runaway child or missing reports where reasons for the disappearance is not clear. Especially with older children, law enforcement should consider the possibility of an online component to all missing child reports.

Private Sector Capability

Private sector technology and support can make a difference in the effort to safeguard and rescue children. Many private sector companies and not-for-profit organizations are working in the field of child safety and human trafficking. However, law enforcement, health professionals, teachers, and public safety officials need help. A whole of society approach is required.

©iStock.com/gorodenkoff

NCMEC and LexisNexis Risk Solutions serves as an example of this essential public-private partnership. Launched in November 2000 and donated by LexisNexis Risk Solutions to the NCMEC in response to a critical need of photo distribution when a child goes missing, the NCMEC uses the ADAM Program to quickly distribute missing child posters to specific geographic search areas, such as a state, zip code, area code, or a combined search area near a city and zip code.

ADAM stands for Automated Delivery of Alerts on Missing Children and is named in honor of Adam Walsh. This program with geo-targeted technology is open to the public for individuals, law enforcement, and businesses to sign up and receive missing child alerts within their specific geographic search area. Increased awareness raised about this program can significantly help in the recovery efforts of missing children. There are over 1.3 million recipients in the program (U.S. only). In partnership with NCMEC, the ADAM Program has helped recover close to 200 missing children and assisted in the recovery of countless others.

The continuation and improvement of information-sharing platforms between public and private institutions, police, federal law enforcement agencies, community, as well as civic and educational organizations are a necessary tool in the fight against child exploitation.

Call to Action – Law Enforcement

A whole of community approach is needed to combat child exploitation with an emphasis placed on education, training, and information sharing. The role of law enforcement is paramount to the successful recovery of children from exploitation and apprehension of individuals and groups responsible for these heinous acts against the most vulnerable of society. Law enforcement continues to adopt a multidisciplinary approach to combat this problem. These five recommendations are critical for law enforcement and public safety professionals to consider:

- *Public education campaigns, training, and public service announcements* – Police officials and investigators should be educated on the issues, scope of problem, and indicators of abuse to be on the lookout for when engaged with the public. An effective training and education outreach campaign established by public-private partnership is the Blue Campaign, which helps raise community awareness of the problem.
- *Global partnerships* – Increased partnerships with domestic and foreign law enforcement and government stakeholders are required to effectively combat this crime. The wide-scale availability and low cost of internet access has in many ways made this a borderless crime.
- *Information sharing* – Collaboration and effective targeted investigations are required to identify, apprehend, prosecute, and dismantle criminal networks that exist for the sole purpose of child exploitation. Jurisdictional issues and the mobility of many sex traffickers can create challenges to investigative and information sharing efforts.
- *Training and investigative techniques* – Continuous training and awareness of the problem is vital. Knowledge of trends and special considerations to identify signs of abuse, special considerations when interviewing a potential victim, and knowing the relevant questions to ask can have a positive influence.
- *Community relationships* – Collaboration and proactive engagement with community leaders, faith-based organizations, business owners, and the public are key to building trust, raising awareness, and increasing reports of suspected abuse.

The epidemic of child exploitation plaguing society is complex with far-reaching consequences for the victims, their families, and the nation. The problem has no borders, and those who perpetrate these hideous acts often operate in the inherent gaps of an open and free society. Law enforcement at all levels along with their global partners pursue these predators both day and night. Obligated to protect the youngest and most vulnerable populations, community efforts are multifaceted and enhanced by knowing the issues, recognizing indicators, and communicating them with potential victims as well as reporting all suspected abuse to appropriate authorities. Broader awareness of the risks leads to earlier recognition of signs of danger and hopefully prevention of a child becoming a victim of exploitation.

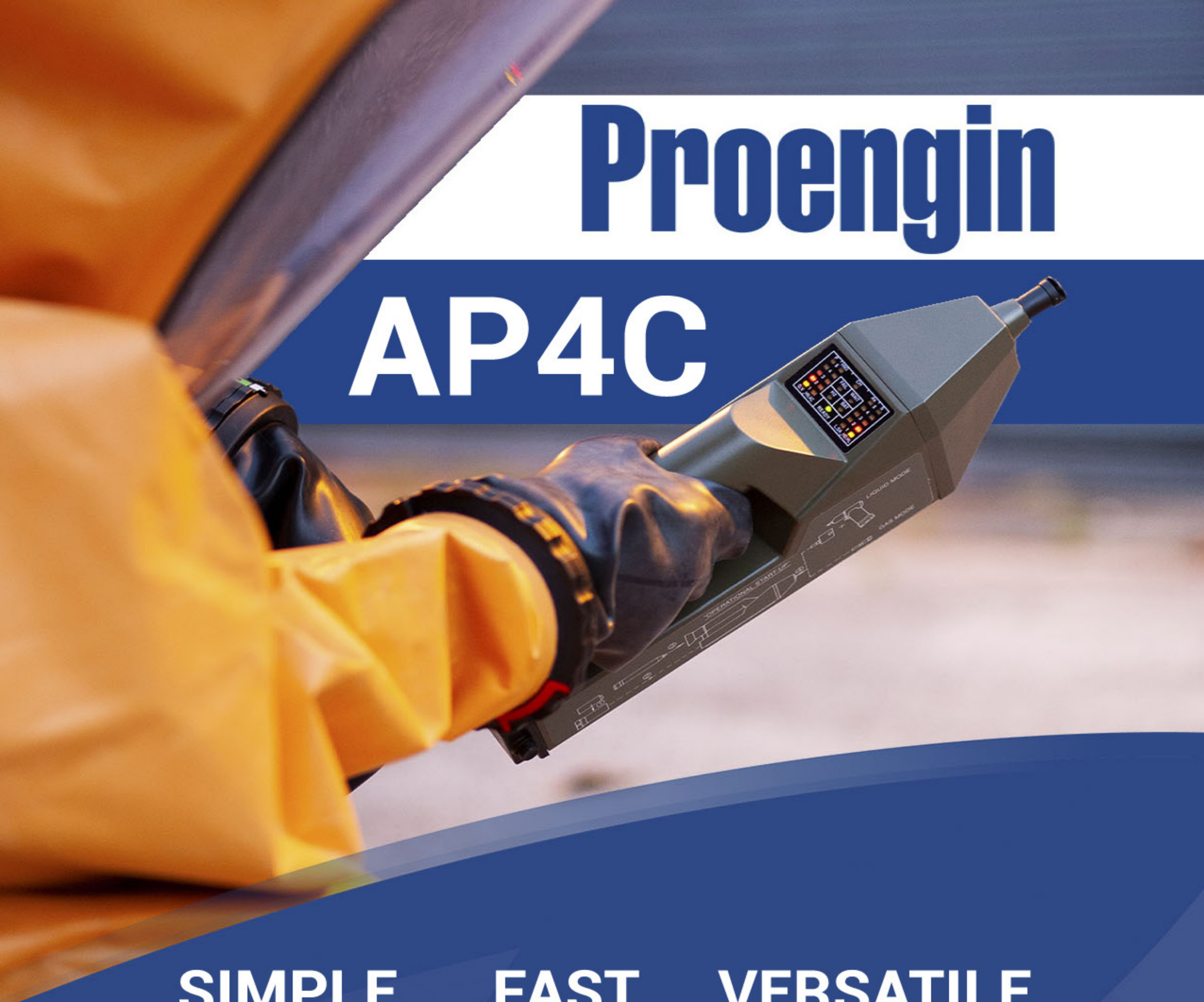
Additional resources not mentioned above:
Prevention Education & Professional Training (National Center for Missing & Exploited Children)
20 Actions for 2020 (Polaris Project)
COVID-19 Resources, Services, and Support – Anti-Trafficking (Administration for Children & Families, U.S. Department of Health and Human Services)
Combating Child Sex Trafficking: A Guide for Law Enforcement Leaders (U.S. Department of Justice)
COPS OFFICE (U.S. Department of Justice)
Combating Child Sex Trafficking: A Guide for Law Enforcement Leaders (International Association of Chiefs of Police)
Crimes Against Children/Online Predators (Federal Bureau of Investigation)

Michael Breslin (pictured) has more than two decades of experience in federal law enforcement and transnational financial and cybercrime investigations. He serves on the Cyber Investigations Advisory Board of the U.S Secret Service and is the strategic client relations director for federal law enforcement at LexisNexis Risk Solutions. Prior to joining LexisNexis Risk Solutions, he served as deputy assistant director for the Office of Investigations for the Secret Service, where he oversaw the planning and coordination of investigative responsibilities. He serves on the Preparedness Leadership Council and is a board member for the National Center for Missing and Exploited Children.

Robert (Bob) G. Lowery Jr. served as the vice president of the Missing Children Division for the National Center for Missing & Exploited Children. He currently provides training for law enforcement on behalf of the United States Department of Justice. He has over 30 years of law enforcement experience having served as the assistant chief of police for the Florissant, Missouri Police Department and commander of the Greater St. Louis Major Case Squad. He was directly responsible for homicide and violent crime investigations in the entire St. Louis Metropolitan Region. He is the author of several law enforcement publications on the topics of investigation of violent crime, homicide, unidentified human remains, abducted and missing children, and missing children with special needs.

Proengin

AP4C



SIMPLE FAST VERSATILE

Chemical weapons & NTAs

HAZMAT & Homemade agents

Quick response

Accurate & Precise

www.proengin.com

Online & Social Media Risks – Protecting Children, Part 2

By Michael Breslin & Robert Lowery Jr.

The nation has experienced unprecedented times due to the COVID-19 pandemic given the requisite need for social distancing and isolation experienced from stay-at-home orders. Daily lives were transformed. For homebound children, this was disruptive and changed daily routines. While at home, children engaged in a variety of safe and supervised activities, such as home schooling, play activities, crafts, games, etc. A side effect of social distancing is temporary physical isolation from many important influences in their lives, such as school and teachers, sports, community organizations, extended relatives, classmates, and friends.

Children are especially vulnerable to victimization, so it is critical to pay attention to the warning signs of sexual victimization and exploitation. Criminals have adapted and exploited public sentiment and vulnerabilities, such as increased availability and free time during the pandemic. The ubiquitous nature of digital systems people use to socially interact have helped children stay connected in times of isolation. It has also resulted in the increased risk of children being groomed and sexually exploited.

Practical Communication & Safety Tips for Protecting Children Online

With the spread of online Child Sexual Abuse Material and popularity of gaming applications, grooming and child sex trafficking are pervasive threats that allow predators to target children. In large part, the internet and social media are a wonderful part of the culture and, in many respects, a primary mode of communication. However, there are those who use these advances for nefarious purposes.

Therefore, parenting must be done in a social media culture. Although seemingly logical, forbidding children to go online is not often a reasonable or realistic expectation. Children know more about using these technologies than many of their parents. Even trying hard to prevent them from using these advancements, today's children are innovative and creative. Many will find a way to get themselves online despite parents' wishes. Following are recommendations for parents:

- Discuss with children (of all ages) internet safety and make them aware of the dangers posed by certain individuals who use chatrooms and social media for illicit purposes.
- Manage and monitor internet use by keeping internet-connected devices in a common room or area of the house in full view and limit the use of cellphones and smartphones.
- Use internet browser controls to filter inappropriate content (sexual, nudity, etc.).

- Consider installing mature content-filtering software.
- Never assume to know who is communicating with children, do not be reluctant to ask questions.
- Talk about what type of information is appropriate to share and what is not.
- Make certain children understand that any image they share will permanently remain on the internet and can be widely distributed, even when shared with a trusted friend.
- Tell children to immediately report to them any inappropriate or sexually explicit conversations, parents and caregivers should then immediately report to law enforcement.
- Keep communications open with older children about the dangers posed by offenders.
- Encourage older children to report inappropriate conversations without being judgmental about the content of the conversations, resist the inclination to blame the child.

Warning About Online Gaming

Millions of children use online gaming platforms, so it is not surprising these platforms are plagued by online predators, who contact and groom children. Inappropriate interactions between adults and children are rampant among popular platforms. Accordingly, Roblox's SEC S-1 filing states:

> *The success of our business model is contingent upon our ability to provide a safe online environment for children to experience and if we are not able to continue to provide a safe environment, our business will suffer dramatically.*

For younger children, parents should consider the following actions to control gaming internet access on devices:

- Review and approve all games before they are downloaded.
- Ensure privacy settings are set to the strictest level possible for gaming systems and devices.
- Remind children to be cautious about invitations from those they do not know to join gaming chat rooms and immediately report any inappropriate conversations.
- Teach kids to protect their identity and not reveal personal information.
- Ensure they know how to block another player who may be aggressive or inappropriate.
- Set controls and know if gaming devices post to another online platform.
- Make sure children know that people they meet on gaming sites are not their friends and may not be who they say they are.

Children's online activity is not always readily apparent. The use of screen names and passwords on various social applications make it difficult if not nearly impossible to retrieve useful information, even when the child's device (smartphone, tablet, or laptop) is available. The sophistication of available countermeasures (to hide content and conversations) using encryption and anonymizers can make the task of uncovering evidence of grooming or sextortion difficult. Law enforcement agencies have availability of resources for forensic evaluations, such as the various Internet Crimes Against Children Task Forces, but this takes up valuable time.

Generally, most parents only have limited knowledge of what social media and gaming applications their children use and with whom they may be communicating. Typically, siblings and the child's closest friends have the most knowledge about such activity. They may even know the screen names and passwords the child uses to access the application or even the screen names of the offenders.

Luring, Grooming, and Sextortion

The dynamics of child abduction and the behaviors of criminal offenders have dramatically changed over the past few years. There are far fewer "stereotypical" abductions (i.e., sex offenders who violently grab children from places like street corners, near schools, or in public parks). Technological advancements – such as AMBER Alerts, cameras on streets and in public locations, smartphones (equipped with still cameras and video recorders), license plate readers, and social media – allow law enforcement to engage the public immediately when an incident occurs. These technologies coupled with an aggressive and robust response when a child is taken can all be credited with the reduction in these disturbing cases.

©iStock.com/Chainarong Prasertthai

Despite this good news, criminals still want to harm kids. In many cases, they have simply changed the way they target and victimize kids. In other words, technology has been both good and bad when it comes to protecting the most vulnerable populations.

Parents must keep open lines of communications with their children and insist that they come to them anytime they are engaged in an inappropriate conversation – regardless the severity. Parents must resist temptations to blame the child. Instead, they must recognize that they are victims and should be treated as such.

Offenders depend on child victims remaining silent out of fear that parents, caregivers, and others will blame and discipline them for inappropriate behavior. They also depend on the child's belief that, if they do not remain silent and obedient, the contents of their conversations (along with their sexual images and videos) will be shared online.

Runaway Children

There are many reasons children run away. Regardless of the reason, the reality of running away presents serious risks the child may not realize or understand. They may be impulsive or believe they would be better off leaving home. They do not have the experience or judgment to always make a sound decision. It is important to talk to children when their behaviors change or they become withdrawn. Children do not always disclose information they are uncomfortable talking about right away. They may not know how to reveal what is troubling them, and they may look for the right time and circumstance to talk. Keeping the lines of communication open is vital. Potential warning signs that runaway children may exhibit include:

- Angry or aggressive outbursts
- Becoming more introverted and withdrawn from family and friends
- Depression or increased anxiety
- Difficulty in school – poor grades, skipping class, behavior issues
- Being secretive about friends or activities
- Having secret social media accounts and spending excessive time online
- Being bullied
- Threatening to run away or staying away from home for extended time periods
- Signs of possible drug or alcohol abuse
- Possessing money or expensive items
- Lying and stealing
- Lacking concern for themselves
- Engaging in self-harming behaviors, including cutting and high-risk sexual behaviors
- Questioning their sexual identity

If a child exhibits any of these indicators, parents should take the following preventative steps:

- Talk to them and try to determine what is bothering them.
- Be honest about changing family dynamics like divorce, financial difficulties, loss of a parent/family member, or a disruptive family environment.
- Listen (rather than lecturing and being judgmental) and make every effort to develop a resolution with the child.
- Be supportive – let the child know they are loved and that running away will not resolve the problem.
- Seek outside resources such as family counseling, therapy, or substance abuse treatment.
- Talk about the importance of protecting their identity (online and offline) and selecting friends wisely.

- Get to know the people who are important to the child outside the family circle.
- Put realistic rules in place and openly discuss why they are important.

If a child runs away, parents should take the following reactionary steps:

- Contact law enforcement immediately, there is no waiting period to report a missing child.
- Provide all pertinent information to law enforcement, including clothing, recent photo, known friends/companions, last time and place child was seen.
- Do not withhold information.
- Make available all wireless devices and technology available.
- Provide all social media accounts/names and cellphone numbers.
- Provide information about custody, including any related issues.
- Provide information about changes in family dynamics or the child's behaviors.
- Inform law enforcement about anyone new or showing unusual attention or interest in the child's life.
- Provide law enforcement with any contacts the child has (phone, text, or in person).
- Be proactive and disseminate information about the child (e.g., fliers, contacting places/ people).
- Stay in touch with law enforcement until the child returns and notify them of their return.

> ***As the first line of defense, parents and caregivers need to be vigilant with social media and gaming applications to protect children from online predators.***

Call to Action – Parents

A whole of community approach is needed to combat child exploitation with an emphasis placed on education, training, and information sharing. Much overlap exists between these themes and should be employed by parents, caretakers, schools, law enforcement, as well as public and private entities. These six recommendations are critical for parents and caretakers to review:

- *Communication and teaching* – Talk with children about the risk and dangers. Establish a plan with children and discuss the plan frequently – reinforce safety tips and good online choices. Remain open to dialogue with children (free of judgment) and provide a means by which they feel safe to reveal if inappropriate or suspicious contact has been made with them.
- *Education* – Know the signs of child exploitation and abuse. Parents need to know and be able to recognize signs if one's child is in danger.
- *Emphasis on safety* – Ensure all children's activities are done in a safe environment. Know who is involved with the children. There is no typical profile of a child molester, so always remain vigilant.

- *Online safety knowledge* – Parents should avail themselves of the many resources and free guides available to help strengthen their child's online safety habits thereby helping to reduce exposure. The use of child protection apps to help counter the increased risks associated with increased time spent online is an option.
- *Planning* – If a child goes missing and is a victim of child exploitation, prior preparation and planning is key. Have a plan (e.g., have a colored recent photo available of the child, know the child's height, weight, etc., know who to call, etc.).
- *Reporting* – The most important thing is to be on the lookout for a missing child. Report any suspected incident of abuse immediately to local law enforcement agencies. Learn about the If You See Something, Say Something campaign. Contact the local FBI field office or file a report with the NCMEC at 1-800-THE LOST or online at www.cybertipline.org.

The problem of child exploitation rips at the very fabric of society not to mention the indescribable agony inflicted on the victim and parent. Child exploitation is a complex problem with many underlying causes and effects. Its prevention is no less a formidable challenge. It is one, however, that all of society must address. The front line of defense begins at home and must be reinforced by all of community. Parents play a vital role in taking a proactive approach in teaching their children about the dangers and preventive steps they can take to help improve their safety.

Additional resources not mentioned above:
Child Abuse and Bullying Prevention Resources for Schools (Kidpower International)
Internet Safety 101
Keeping Children Safe Online (U.S. Department of Justice)
Keeping Children Safe Online During COVID-19 (U.S. Department of Justice)
Protecting Children During COVID-19 (Global Partnership to End Violence Against Children)

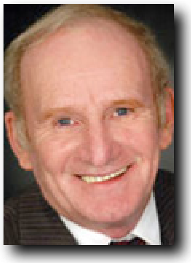
Michael Breslin has more than two decades of experience in federal law enforcement and transnational financial and cybercrime investigations. He serves on the Cyber Investigations Advisory Board of the U.S Secret Service and is the strategic client relations director for federal law enforcement at LexisNexis Risk Solutions. Prior to joining LexisNexis Risk Solutions, he served as deputy assistant director for the Office of Investigations for the Secret Service, where he oversaw the planning and coordination of investigative responsibilities. He serves on the Preparedness Leadership Council and is a board member for the National Center for Missing and Exploited Children.

Robert (Bob) G. Lowery Jr. served as the vice president of the Missing Children Division for the National Center for Missing & Exploited Children. He currently provides training for law enforcement on behalf of the United States Department of Justice. He has over 30 years of law enforcement experience having served as the assistant chief of police for the Florissant, Missouri Police Department and commander of the Greater St. Louis Major Case Squad. He was directly responsible for homicide and violent crime investigations in the entire St. Louis Metropolitan Region. He is the author of several law enforcement publications on the topics of investigation of violent crime, homicide, unidentified human remains, abducted and missing children, and missing children with special needs.

Fixing America's Healthcare Supply Chain

By James Rush

The buildup to World War II illustrated the negative effect that huge wartime demand for medical supplies, equipment, and pharmaceuticals had on public and private healthcare systems in the United States. After the war, the Defense Logistics Agency (DLA) began building and pre-positioning federally owned medical materiel in storage depots domestically and materiel management centers in the European and Pacific theaters of operations. Collectively, these inventories were named war reserve materiel (WRM) and consisted of billions of dollars of medical materiel. The WRM was designed to provide wartime start-up supplies until medical materiel manufacturers could ramp up production to levels capable of supporting both wartime and civilian healthcare needs simultaneously. The medical WRM was also used to provide medical support to contingencies and humanitarian assistance missions both at home and abroad.



In order to maintain medical supplies within shelf-life parameters, armed forces healthcare facilities were required to use WRM supplies to the maximum extent possible in order to conserve the DLA's investment in inventory and maintain its supplies and equipment ready for deployment worldwide. When the 1991 Gulf War broke out, pre-positioned medical materiel in Europe and at U.S. depots supplied the initial start-up inventories for medical facilities set up in the Middle East. The WRM system worked as advertised, relieving much pressure on the healthcare supply chain. However, almost immediately after the Gulf War, American politicians decided to draw down WRM inventories both at home and overseas. It was part of what was called a peace dividend.

Lessons From COVID

The current pandemic laid bare the shortsighted approach to medical materiel management. The just-in-time supply chain broke down, and there were no "just-in-case" inventories to sustain healthcare services. This left healthcare providers without much needed personal protective equipment and many of the supplies and equipment needed for pandemic care and everyday patient services.

©iStock.com/http://www.fotogestoeber.de

One idea being recommended for decades is a medical materiel management system that functions like the Strategic Petroleum Reserve for petroleum products. Using this model, the government would purchase and own reserve inventories of medical materiel, ready to supply any mission the government directs during emergencies.

Urgent Action Plan

The following actions would re-establish the healthcare supply chain just-in-time inventory model:

1. The federal government should direct the DLA to institute a federal Disaster Reserve Materiel (DRM) program. This program should be large enough to supply and sustain the U.S. healthcare and public health systems for 90 days during future disasters, or until medical manufacturing can ramp-up to meet the new demand for product.
2. Re-institute the DLA's Directorate of Medical Materiel as the executive agent for DRM oversight. However, instead of returning to the former depot system, use major U.S. healthcare distribution companies to manage DRM in storage.
3. Reinvigorate the National Disaster Medical System (NDMS) and establish disaster reserve materiel supply lines between DLA, prime vendors, and NDMS partner hospitals, and eventually connect other healthcare entities on a voluntary basis.
4. Select one prime vendor for each DRM class of supply (medical/surgical, pharmaceutical/biologics, and medical equipment) to manage the government-owned DRM and to conduct quality control functions and to maintain all medical materiel within shelf-life parameters.
5. Demonstrate the DRM system's capability and capacity to rapidly move DRM materiel to U.S. healthcare organizations using existing distribution networks during NDMS exercises or actual disasters.
6. Discourage healthcare organizations from building their own inventories in order to enable DRM prime vendors to develop highly accurate inventory demand models that closely correlate with actual materiel usage.
7. Restore the pre-COVID healthcare supply chain in a manner that uses a "just-in-time" inventory model for everyday health services and very deep and resilient DRM inventories for use in future large-scale disasters … and, yes, even a future pandemic.

By instituting a federal DRM system, the U.S. healthcare supply chain will be both economical during normal times and resilient enough to expand to meet any future disaster requirements for medical materiel.

James M. Rush Sr. has over 45 years of healthcare administration and community emergency management experience in the U.S. armed forces, the U.S. public-health community, and the nation's civilian healthcare industry. He served as the Region III project officer for the National Bioterrorism Hospital Preparedness Program, and the CDC's National Pharmaceutical Stockpile, always dedicated to assisting healthcare and public health organizations prepare for "all hazards" events and incidents. He is author of, among other published works, the "Disaster Preparedness Manual for Healthcare Materials Management Professionals," and a self-published book "Unprepared."

FilmArray