



Emergency Notification Systems: Safeguarding the Nation's Critical Infrastructure

The U.S. Department of Defense utilizes network-centric emergency alerting systems that promote effective emergency response.

By Guy Miasnik

In a perfect world, budgets would be unlimited and protecting our nation's critical infrastructure would be easy. But the reality is many of our nation's most important assets are outside of the federal government's protection and potentially are at risk. In fact, as much as 90 percent of the critical infrastructure is in the hands of the private sector and state and local governments.

Organizations with very real budget constraints are responsible for maintaining and protecting the nation's electricity, ports, emergency response, financial systems, police, oil supplies/distribution, telecommunications, transportation and sewer and water services. While the federal government has begun taking a more active role in protecting the nation's critical infrastructure, a large burden remains with corporations and state and local governments. In the face of increasing threats, what cost-effective options are available for those tasked with safeguarding our infrastructure?

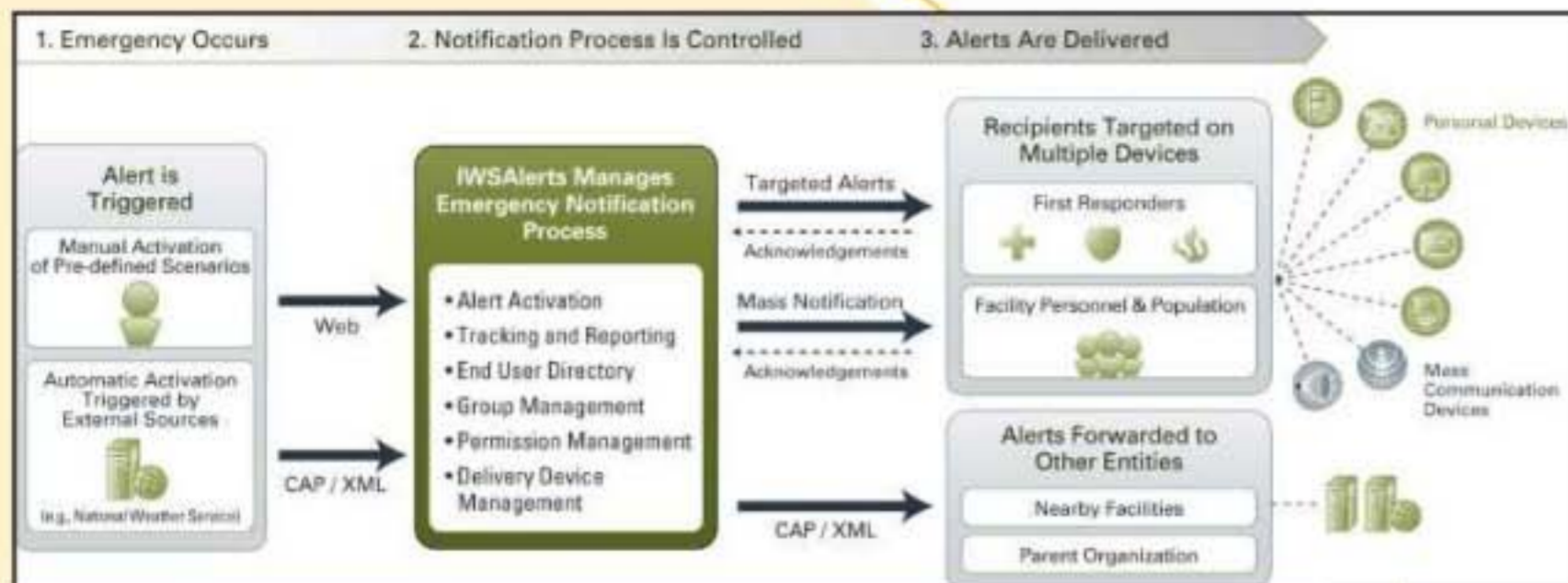
One option is to look to the U.S. Department of Defense (DoD) for ideas. Numerous systems have been employed in the DoD that can have positive outcomes in protecting the critical infrastructure. The DoD has the resources to successfully implement programs and technologies designed to protect its personnel, facilities and the public. Organizations can learn from the DoD's best practices without having to endure the numerous trials and tests otherwise necessary to identify effective protection measures.

DoD widely utilizes network-centric emergency alerting that improves their situational awareness and helps promote effective emergency response. This type of technology is highly relevant for any organization tasked with protecting critical infrastructure facilities commonly covering large geographic areas with personnel dispersed throughout.

Focusing Limited Resources

One might assume the DoD's primary security mechanisms are its combat weapons systems. Not true. The DoD's primary protection instruments exactly are what it would be for any facility – command and control tools that promote situational awareness for fast and effective decision-making, and that enable quick communication and notification to personnel.

In a recent study commissioned by the Commander of Naval Installations to evaluate technology systems' return on investment for promoting force protection and physical security, of more than 20 technologies studied, the top two capabilities identified were decision support systems and area-wide notifications. Decision



support helps emergency managers assess situations and determine the appropriate plan of action. Area-wide notification enables the emergency managers to communicate with first responders and all affected personnel to supply appropriate emergency information, provide required response actions and collect personnel status.

The DoD aggressively is deploying technology to support decision-making through situational awareness, and they also are using network-centric emergency notification platforms to quickly alert personnel with clear instructions for action once emergency situations are identified.

Promoting Decision Support through Situational Awareness

In the last decade, DoD personnel responsible for emergency response faced the same problems encountered throughout the emergency response industry. With the burgeoning “information age” came the inevitable phenomena of information overload. The avalanche of irrelevant, inaccurate and delayed information fragments made it difficult to see the forest for the trees, reducing the ability to react quickly to the more relevant information. Situational awareness became compromised.

To mitigate the information overload, military installations turned to technology to quickly identify the most relevant information and automatically trigger the appropriate response.

For example, the United States Strategic Command (USSTRATCOM) Global Operations Center began using technology to its advantage to improve situational awareness through information monitoring and targeted alerting. USSTRATCOM deployed a network-based, user alerting system to monitor a set of data sources and content feeds for strategic threats and conditions (anything from a missile silo opening to a tornado approaching) and deliver real-

time alerts to decision makers based on their roles, self-subscriptions and need-to-know status. These notifications drive situational awareness and allow decision makers to effectively manage critical events and emergencies in a timely manner, especially under crisis conditions.

Filtering technologies can look for triggers within a facility’s physical and cyber landscape, and importantly, they also can filter data feeds from outside sources such as the National Weather Service, news feeds or organizations such as the Department of Homeland Security. Using filtering, organizations can get a more accurate view of their environment and the emergency situation, allowing them to better respond and take the appropriate actions.

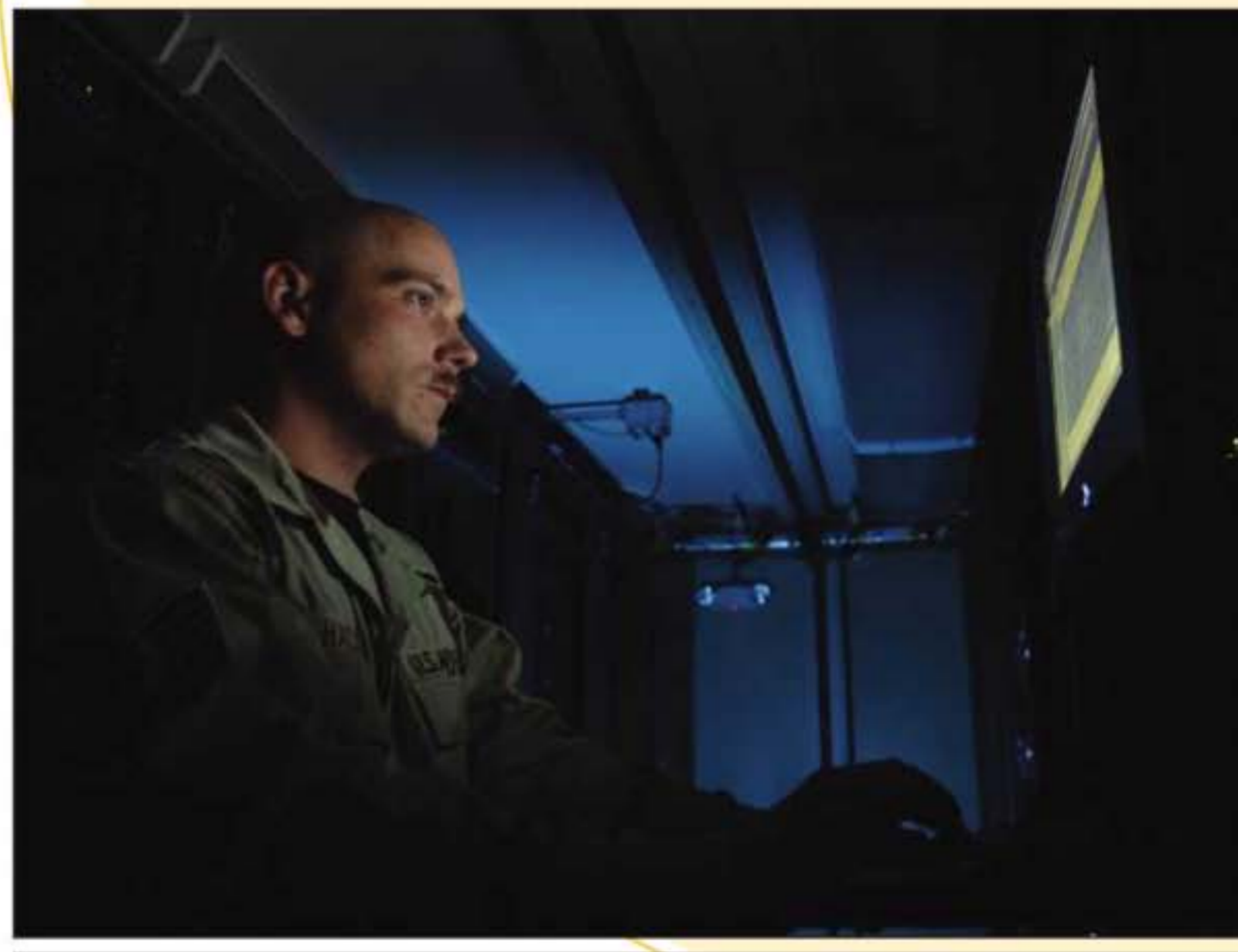
Once an organization builds a solid foundation for information discovery, it should focus on the second critical element of emergency notification – rapid information dissemination.

Real-Time Alerting to Targeted Groups

When decision makers become aware of a situation and decide on the appropriate course of action, the next step is to alert personnel. Network-centric alerting technologies help emergency operations centers within the DoD reach tens of thousands of recipients by transforming the IP network into a physical alarm system in times of emergency. Recipients can be reached within seconds, regardless of their physical location, whether it be via computers, personal digital assistants (PDAs) and land line and cell phones. Highly-targeted,

personalized information is sent to different groups, of recipients based on criteria such as their roles, functions or location. For example, firefighters would be sent details and location of a fire, whereas other personnel would be sent evacuation instructions and routes as well as a query to their current status.

Because the alerts are sent through the IP network to network-connected devices, organizations can provide detailed instructions for action within seconds to all applicable personnel. Operations centers can predefine potential scenarios and decide who should be doing what to respond to the situation. If the scenario actually does occur, with a single click of the mouse, thousands of people can be alerted, each receiving detailed information about what they should do, where they should go and what safety gear they might need. While most organizations within the critical infrastructure don’t necessarily have thousands of employees, reacting to critical situations still requires quick access to information. The same type of network technology that benefits the DoD can benefit a power plant, water filtration plant or



MASTER SGT ROBERT W. VALENCA

a port by disseminating emergency information immediately to all impacted personnel wherever they are located and through a whole host of communication channels. In parallel, communications can also be sent externally to local first responders, neighboring communities, or even the applicable federal agencies.

The alerts are controlled from a single console and are consistent regardless of the delivery devices used. For example, desktop alerts are in the form of intrusive audio-visual pop-up windows, while phone calls are delivered with computer-generated text-to-speech voice response calls. Both describe the situation, the threat level and instructions for action as well as recipient response options. Desktop alerts are the fastest and most scalable message delivery mechanism for personalized and mass notification - capable of reaching tens of thousands of people in seconds. Telephony and text messaging provide for flexibility in reaching personnel not at their desks, but due to capacity and message length limitations respectively, these are typically used for targeting specific groups.

Emergency operators can centrally create, manage and send alerts to any computer or device using a standard Web browser, without the need for any software to be installed on the operator's station. This vital capability gives emergency notification teams the ability to use alternate locations and workstations as a fail-safe method should the operations center become inoperable.

Alerting systems must include the appropriate safeguards to ensure only authorized personnel can launch alerts. Operator permissions can be created to provide a range of different access rights, such as controlling the notified personnel, to determining the type of alerts to be sent.

Topping the list of important capabilities provided by network-centric emergency alerting systems is the ability to track alert recipient responses. When an emergency occurs, there is nothing more important than taking care of personnel. Not only does network-centric alerting help organizations promote employee wellbeing by arming them quickly with instructions for action, it also allows command centers to track personnel responses to alerts. Using their closed-loop capabilities, net-centric systems can ask for a response from a recipient to determine personnel's status (OK, hurt, etc.), location and ability to act. This provides the decision makers with a much needed picture of the status of their people and who is available to help address the emergency. Traditionally, such processes would have taken hours or days, but now a clear picture of personnel status is available in near real-time.

Drawing Parallels from the Department of Defense

Today most organizations rely on long-standing alerting methods such as sirens and public address sys-

tems to warn of approaching danger. In light of the potential loss of lives and catastrophic property damage, we must leverage available technology to equip emergency operation centers and first response teams with the information they need to ensure rapid and effective results in times of crisis.

Most organizations will never have a fraction of the DoD's

NEWLY EMERGING TECHNOLOGIES ARE HELPING OPERATIONS CENTERS PLAN AND REACT MORE EFFECTIVELY TO EMERGENCY SITUATIONS.

resources, but they can leverage the work it's already done to identify and prioritize the appropriate areas of investment. Ports can benefit from the technologies the Navy deploys to protect its installations. An airport can learn from the best practices used by the Air Force to protect its bases and landing strips. They face many of the same threats - both from nature, accidents and terrorist attacks.

By promoting situational awareness and rapid information dissemination to targeted audiences, newly emerging technologies are helping operations centers plan and react more effectively. The resulting situational awareness - the ability to know what is happening around you - is instrumental in the decision process and resulting response plan. Real-time, network-centric notification technologies facilitate targeted alerting to make sure those most impacted by a threat are prepared for an effective response.

It's time to take a cue from the DoD to make sure the nation's infrastructure is properly secured.

Guy Miasnik is the president and CEO of AtHoc, which creates enterprise-class, network-centric alerting systems for emergency notifications, force protection readiness, situational awareness and critical communications. AtHoc's technology is widely used across the U.S. Department of Defense. Miasnik has over 18 years of experience in the IT sector with specific expertise in C4I (Command, Control, Communications, Computers and Intelligence) solutions and technologies. He can be reached at guriasnik@athoc.com.



MC3 MICHAEL A. LANTION