



[SUBSCRIBE](#) || [MEDIA KIT](#) || [READER SERVICE](#) || [CONTACT](#)

Putting the Pieces Together

No single technology will achieve border protection if it's deployed only as a standalone system

By David M. Stone



WITH heightened concerns about international terrorism, increased attention is being placed on techniques to enhance the security of U.S. borders. There is a focus on achieving the most effective protection while optimizing the efficiency of security personnel and other resources.

So-called smart technologies are currently being developed that offer the potential to make significant improvements in border security today and in the future. As this technology is considered and applications are tested, the need for a comprehensive, connected network is apparent.

The U.S. border is a vast territory that includes thousands of miles of land and sea borders combined with many crossing points, ports, railway terminals, airports and other gateways to and from the country. No single technology or even a cluster of advanced technologies will result in a breakthrough in overall border protection efficiency if it is deployed only as a standalone system that surveys a specific territory. What is critical for taking security to the next level is aggregating information from various sources within a single network that provides total situational awareness of the borders.

Real-Time Domain Awareness

The Department of Homeland Security and the Department of Defense commonly use the phrase "total domain awareness" in describing the aim of protection and surveillance initiatives. To achieve the desired level of awareness, information and intelligence from various locations needs to be fully integrated so that critical cueing tasks can be sent to responders for their immediate attention.

To achieve a comprehensive understanding of what the "domain" -- such as a border -- should be, a normal environment has to be mapped out in detail to serve as a baseline so that observers can detect and respond to anomalies. On an ongoing basis, command teams receive a variety of information through various reports, intelligence and sensors in order to form what the military often calls the Common Operational Picture (COP). Once this picture is formed, the opportunity to detect anomalies and alert responders is possible.

Current DoD activities overseas provide a good model for describing this concept. In areas where the DoD is engaged in military actions, real-time domain awareness of a border or other areas can involve such technologies as unmanned aircraft with infrared cameras, radar, satellites, blimps and other sensors. These efforts continue 24/7 in all

No single technology or even a cluster of advanced technologies will result in a breakthrough in overall border protection efficiency if it is deployed only as a standalone system that surveys a specific territory.

AltaVista
BabelFish
To translate this page, click a flag!

Flags for: China, Germany, Japan, South Korea, France, Italy, Russia, Spain

[Print this Page](#)

[Click here](#) to email this page to a friend.

conditions. All of this information is networked into DoD command centers, where it is analyzed in combination with current information from ongoing intelligence efforts.

[Ads by Google](#)

For example, if convoys of trucks usually pass a particular spot during the day, and one day, there are none, that is an anomaly. If human activity is not normally seen in an area during the night, and groups of people are seen gathering, that is an anomaly. Intelligence can give indications of why these anomalies are occurring at a given time to help coordinate the best response.

[Alarms](#)

Looking for Locksmiths? Find a great one near you now.
siliconvalley.citysearch.co

Similarly, networked technologies and sensors can provide real-time domain awareness for U.S. borders. Combining legacy systems with advanced smart technologies can take security to the next level. This process is evolutionary, not revolutionary. For example, smart technologies in the video arena already can be programmed to detect anomalies and send a video clip of an incident, along with other sensor information, to a responder via pagers, cell phones, beepers or radios.

[EBS-Nationwide OT Jobs](#)

Entry level to supervisory jobs All locations and settings
www.EBSHealthcare.com

The many types of information -- such as voice, data and video -- eventually can be integrated and distributed through a common network. The integrated information is then available to command centers and designated responders around the clock for true situational awareness. Of note, over a period of time, the review and analysis of this integrated information product provides key watch team leaders with an expert knowledge of the domain that is needed for true domain awareness.

[Coordinated Response](#)

A common network also results in a coordinated effort among the many agencies that share responsibility for various aspects of border protection. Customs and Border Protection has the lead role for border security. Monitoring people, vehicles, aircraft and sea craft -- along with materials that enter and leave the country -- is a monumental task. It also is a mission shared by the CBP with many other federal agencies, state and local authorities, and the private sector.

[Tech Jobs at Dice](#)

Search 70k+ tech jobs from top companies. New jobs posted daily.
www.dice.com

The development of a single network can help coordinate the efforts of this diverse team, increase overall efficiency and effectiveness, and ensure there is a unity of command.

[ADT@: Official Site](#)

Burglary, Fire and Carbon Monoxide Protection from ADT Home Security.
www.ADT.com

A variety of sensor information linked together and fed into a common network -- such as aerial surveillance, ground video, radar, chemical detectors and behavior recognition software -- also can be pre-programmed to send an alert or elevate it to an alarm. At the same time, if many responders were necessary, that response could be coordinated to the point of directing responders to a specific location with a specific task. Personnel can be more productive and deployed with greater efficiencies.

[Advertise on this site](#)

Advances in wireless mesh technology add an exciting dimension to the border security solution, and the potential for real-time detection and response will be enhanced by further development of this technology.

[Sensors and Other Surveillance Technology](#)

An array of sensors can link into the border security network, providing a continuous stream of information. These technologies include satellites, unmanned air vehicles and blimps for aerial surveillance. Increasingly, advanced technologies are being developed and applied in surveillance, including even more sophisticated unmanned air vehicles, chemical sensors and software that analyzes video, radar and infrared images to identify anomalies.

Technologies such as behavior recognition software and backscatter/catscan devices can be particularly useful for indicating anomalies. For example, behavior recognition software available today can recognize a human being, distinguish how many people are in the camera view and spot whether their actions are unexpected or undesirable in a given environment. Algorithms can be written to identify specific behaviors, types or sizes of vehicles, packages, objects or pieces of luggage, and can be fine-tuned to each camera across a border area.

Backscatter devices and catscan technologies reveal the density of the contents of vehicles, crates and containers. Software capabilities provide a color-coded chart to indicate the possible contents, which can be rapidly compared to a log of stated contents to check for anomalies.

Technology has the advantage of improving detection accuracy while also improving throughput and efficiency. While security procedures like physical searches of cargo at ports and people at airports impedes schedules, the real-time scanning and surveillance techniques can significantly speed up the entire security process.

If individual detection technologies such as sensors for nuclear material are too expensive or physically impractical to install in large numbers, such devices can be deployed and networked on a border-wide scale. For example, at ports of entry, relatively small and fully networked nuclear detection devices can be placed on actual crane hoist attachments that are used to load/offload containers so that the normal business process is not interrupted. This type of seamless solution is the optimum approach to enhance security and not interrupt the flow of goods and services.

Role of Intelligence

As a nation considers investments in border security technology, the proper investment in intelligence is an extremely valuable element to any strategic security plan because it allows us to play offense, not just defense.

If a terrorist "archer" has 10 "terrorist arrows," it may take many more resources to attempt to stop all 10 terrorist arrows (treacherous people, dangerous weapons or nuclear materials) at the U.S. border than to stop the archer overseas before the arrows are launched. The objective must definitely be to allow for the capture of the enemy archer before the arrows are launched, not after.

This approach however, calls for intelligence sources that enable the United States to take the fight to the enemy in an effective manner. Networked intelligence is the most powerful tool in stopping the arrows from being launched. The product of this network can provide information about locations, times and activities that can help focus border protection efforts for greatest efficiency. Technologies and software that allows for the transformation of intelligence data into accessible and useful knowledge is key to this effort.

Intelligence networking across agencies and departments is an enormous challenge, and it is a matter that is being studied closely today at all levels of government. Ultimately, even the most advanced technology is only part of a comprehensive border protection solution. Networked intelligence is mandatory if we are to create the real-time domain awareness needed by decision makers to take informed, decisive and effective action.

Leading the Way

Threats from international terrorism are bringing increasing attention to the issue of U.S. border protection. The growing number of highly advanced detection and surveillance technologies offer excellent solutions. However a real-time, comprehensive, overall picture of the U.S. border can only be achieved when all of this data is integrated and analyzed as a whole.

Networked data, including intelligence products from a wide range of sources, can provide the highest level of domain awareness. Establishment of norms; detection of ambiguity; continuous monitoring; integration of voice, data and smart video inputs; wireless mesh networking; seamless nuclear detection processes in our ports of entry; information gathering that is distilled into knowledge; and real-time coordinated responses that are cued from command centers are all key to the future development of the most efficient and effective border protection for our nation.

The technology is there to support us. It is up to our leaders -- both public and private -- to now lead the way.

This article originally appeared in the December 2005 issue of *Security Products*, pgs. 49-51.

David M. Stone, rear admiral, Navy (Ret.), is the former assistant secretary of homeland security for the Transportation Security Administration. He currently serves on the advisory board for

Vidient Systems Inc. Stone is a 28-year career Naval officer and served from 2002-2003 as TSA's first federal security director at Los Angeles International Airport.



[Home](#) | [Features](#) | [News](#) | [Products](#) | [NEW Employment Forum](#) | [2006 Product Directory](#) | [Links](#) | [Card Deck](#)
[Search](#) | [Subscribe](#) | [Free Newsletter](#) | [Free Product Info](#) | [Advertising](#) | [Contact Us](#)

© Copyright 2006 [Stevens Publishing Corporation](#)
5151 Beltline Road, 10th Floor, Dallas, Texas 75254
Reproduction in whole or in part in any form or medium without express permission
of Stevens Publishing Corporation is prohibited.
[Privacy Policy](#) | [Reprints](#)
Contact the [webmaster](#)