Brainlike Homeland Security Relevance

Brainlike, Inc. offers superior monitoring technology to meet key homeland security needs, including the following:

- Bio-terrorism early warnings. The best response to bio-terrorism will be preventing attacks from reaching epidemic proportions, which in turn will require detecting unusual disease patterns at once. Delivering early warnings will require automated computer networks that will deliver comprehensive disease incidence data to central locations in real time. Converting incidence data to *valid* early warnings will also require Brainlike methods to separate true disease outbreak leading indicators of from the many false indications that could be misinterpreted as such.
- Unexpected airport activity. Suppose that several unexpected activity indicators were recorded and supplied to an airport security operations center every few minutes. Such recordings might include the average time spent inspecting each piece of luggage and the average time spent screening each passenger at the ticket counter — the kind of information that could have pointed toward terrorist activity at Logan Airport on the morning of 9/11. Then subtle signs of unusual activity could be detectable using Brainlike technology and preventive action could be initiated accordingly. On the morning of 9/11, nine highjackers were briefly detained and screened as potential threats at the Logan Airport ticket counter. Could Brainlike technology have shown that nine strange things were happening at once and prompted immediate preventive action? Perhaps.
- Unexpected traffic activity. Suppose that a variety of surface, sub-surface, and airborne sensors were supplying correlated activity information to a traffic monitoring center. In that case, Brainlike technology might detect subtle changes that would otherwise be undetectable, so that preventive action against terrorist threats could be initiated accordingly.
- Unexpected computer network activity. Products using Brainlike technology have already been delivered that identify subtle computer problems under dynamic operating conditions. Under contractst with ARDA, NSA, and the Navy, Brainlike, Inc. has investigated the use of similar products to prevent sophisticated cyber attacks.
- Unexpected power consumption. Suppose that CIA reports uncovered a terrorist plot to launch a laser-based attack on a passenger jet landing at a U.S. airport. Anti-terrorism units might then be able to pinpoint and neutralize the attack if they could quickly recognize unexpected increases of energy usage in the region. In closely related incident monitoring settings, Brainlike technology has been shown to add substantial precision and lead time value.
- Reduced anti-terrorism operating costs. Regional, state, and national governments are acutely aware that anti-terrorism operating costs can be enormous. Key to cutting such costs is reducing false alarms. False alarm response costs can be so large that officials may be forced to ignore alarms entirely. Los Angeles County electronic break-in alarms is a recent case in point. High costs also result from major time and effort associated with delivering effective monitoring systems. The kind of effort needed to anticipate all possible attack contingencies is simply out of the question, because some of them haven't even yet been

imagined. Brainlike monitoring offers huge cuts in total operating costs along both false alarm and product cost reduction lines, by continuously learning what to expect.

- **<u>Tragedy prevention</u>. Brainlike technology adds huge value by identifying developing problems immediately so that action can be taken to prevent costly incidents of tragic proportions.**

Figure 1 shows a ticket counter monitoring display panel that suggests an intriguing possibility: if this panel had been installed and integrated with Brainlike surveillance technology on the morning of 9/11, the tragedy might have been prevented. Each light in the display panel represents activity at a particular ticket counter during a 30 minute period. If passengers were being processed at that ticket counter in an unusually careful way, a red light would be displayed. The pattern of red lights in Figure 1 has been created to show the kind of ticket counter activity that reportedly took place prior to the 9/11 highjackings. In particular, nine of the 9/11 terrorists were retained for an unusually long time at ticket counters during check-in, as indicated in the figure by 0530 red lights at United and American airline ticket counters. If this display had been available at a Logan Airport surveillance operation center (SOC), the 9/11 tragedy may not have gotten off the ground.

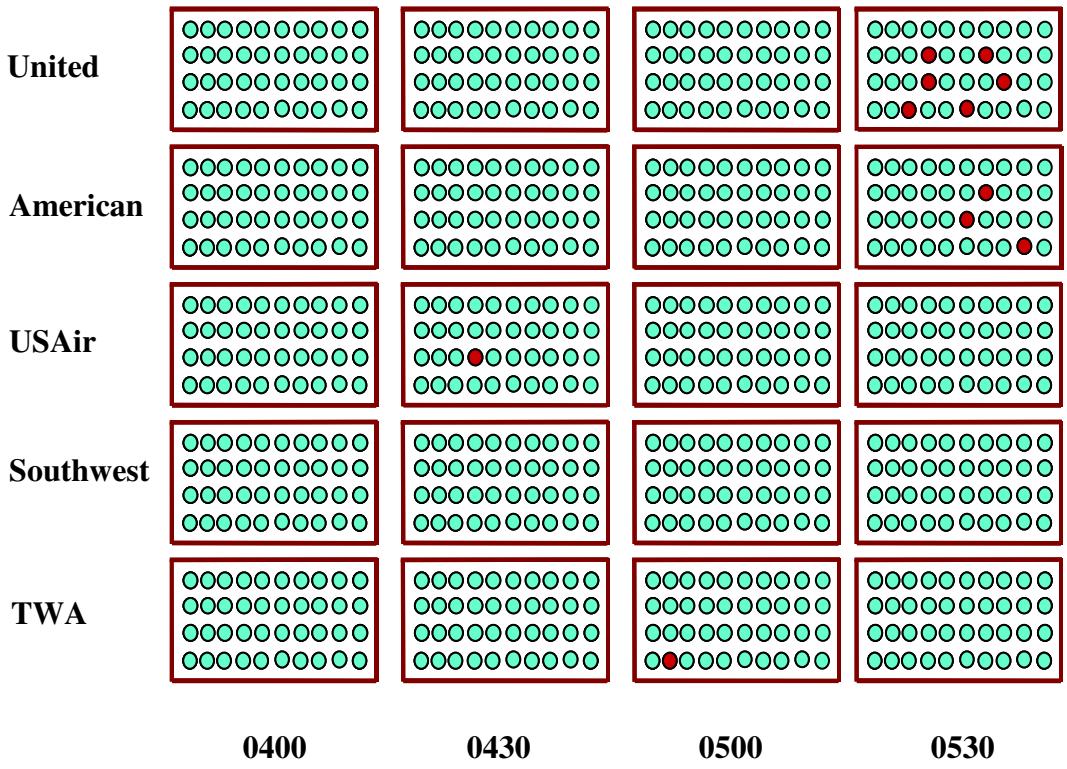

Figure 1. Airport Ticket Counter Activity Monitoring

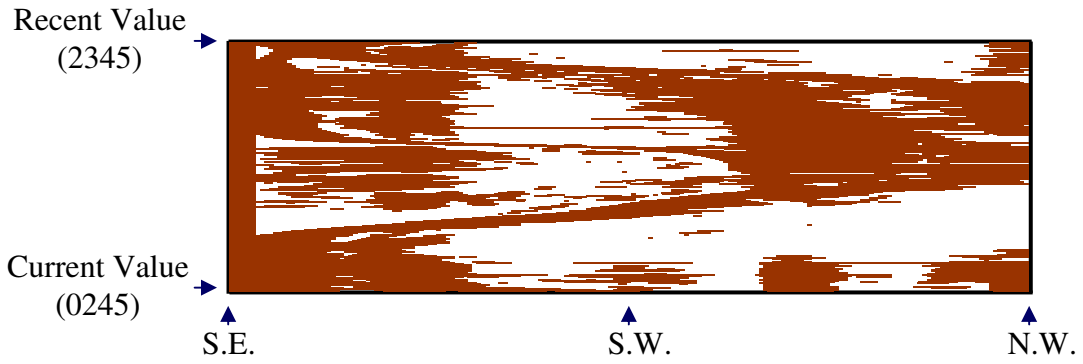

Figure 2. Conventional Traffic Monitoring

The Figure 1 display was not deployed on the morning of 9/11, partly because officials weren't aware that such a tragedy could happen, but also because they didn't know that such a display was viable. Since 9/11, awareness has been raised, SOC networks have become feasible,. and Brainlike advances have made the display of *valid* red and green lights viable.

Figure 2 illustrates what surveillance officials are up against using conventional monitoring technology, even in cases where SOCs are up and running. The figure shows a conventional sonar display of shipping activity in San Diego harbor during a three hour period. The figure is dominated by routine activity, including ships entering and leaving the harbor as well as vessels anchored outside the harbor. Embedded in the figure is a set of sonar blips indicative of a small terrorist submarine entering the harbor. Although the conventional sensing system that generated the figure was tuned to show the blips as clearly as possible, the blips are hidden

Figure 3 shows a display based on exactly the same data that produced Figure 2. The sonar blips representing intrusive activity are clear from Figure 3 as opposed to being hidden in Figure 2, even when the viewer knows where to look for them. The key difference between the two displays is that conventional monitoring produced Figure 2 without continuous learning, while Brainlike monitoring with continuous learning produced Figure 3. Moreover, the Brainlike system that produced the Figure 3 display required no prior modeling or data analysis. The system simply began learning at the beginning of the three-hour period shown and was able to distinguish unexpected signals from routine signals after only a few minutes, all automatically.

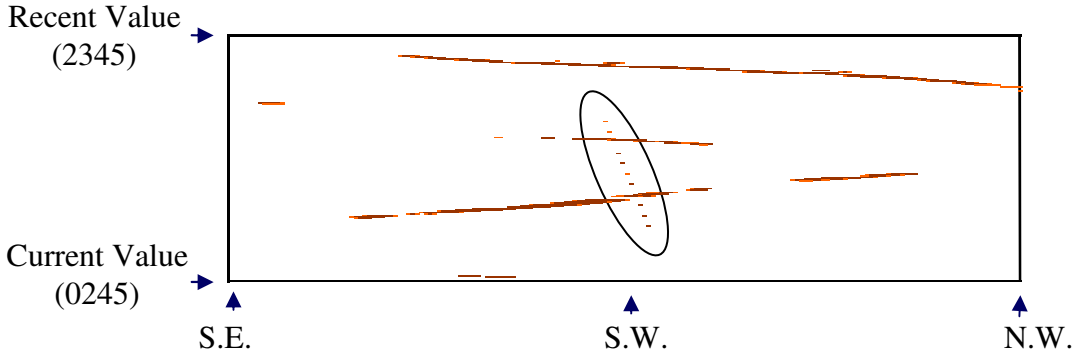

Figure 3. Brainlike Traffic Monitoring

While this report outlines the relevance of Brainlike technology for HLS, its real strength comes from years of prior effort that have produced the world's best monitoring technology. The distinct Brainlike Advantage, its proven added value in many applications, its successful development of related commercial products (see www.Netuitive.com), and its huge overall savings are second to none.