Policy, Practice, and the Search for Alpha

Robert Josefek

SCIENCE AND TECHNOLOGY, STRATEGY AND POLICY

If there were a scale to measure the level of abstraction associated with science, technology, strategy, and policy, we could think of science and technology at one end and strategy and policy at the other. While scientists and technologists often must work to understand and manipulate very small, detailed aspects of a problem (like searching for the value of alpha in a formula that will optimize coverage by a radio signal), policy-makers often attend to the large, macro aspects (perhaps deciding who can use available radio frequencies and for what purposes). While both ends of the spectrum are important, my observation is that it is sometimes a challenge for these groups to understand and best benefit from each other. Yet innovations in science and technology can enable policy options that were not previously available and policy goals can drive scientists and technologists to find ways to reach heretofore-unobtainable objectives. To work well, these diverse worlds need to work together. It is with that idea in mind that we present a set of papers recently judged best-in-track and best-in-conference at the 2010 Institute of Electrical and Electronic Engineers (IEEE) Homeland Security Technology (HST) Conference, the tenth annual meeting of this group.

NATURE OF THE RESEARCH

The work presented at the conference falls under the science and technology strategy for ensuring long-term success of the homeland security enterprise. As a whole, it represents a multi-disciplinary, cross-functional, multi-faceted approach characterized by complexity and detail. As individual researchers present their work, there is clarity for scientists and professionals working within that domain.

Yet it is the diversity of work that is most remarkable. Some of the research presented at the conference focuses primarily on preventing or disrupting terrorist attacks; some on protecting people, critical infrastructure, and key resources; and some on supporting response and recovery from incidents. Most of the science and technology research presented, while very specific in its design and application, addresses multiple broader strategies. For example, the work on fast neutron radiation detection supports prevention, disruption, and response strategies.

Some of the work is within a well-defined discipline while other research brings together science and technology from multiple domains. The work using meshed networks to control unmanned aerial vehicles illustrates this type of convergence as it relies on developments in sensors, aircraft, and publicly available communication technologies. In a similar manner, some of this research extends beyond a single process to address several processes that are part of homeland security strategies. For instance, work to automate information sharing and compliance at fusion centers includes communication, interoperability, and other processes that impact situational awareness.

Some of the work focuses on a single type of threat. Consider the focus on intrusion detection by fence breach addressed by intelligent acoustic and vibration recognition and alert systems that would be useful at international borders, airports, and other critical infrastructure facilities. Other developments have the potential to provide assistance across a range of threats and hazards. For example, research into how to augment the U.S. Coast Guard's differential GPS (DGPS) broadcast system with

emergency information could be useful in response and recovery efforts whether the incident is caused by high-consequence weapons of mass destruction or other forms of violent extremism, a major accident, natural hazard, or smaller scale terrorism.

The result of this work is the kind of multidisciplinary, cross-functional research that benefits the broad concerns of homeland security and its multitude of strategies. Yet real-world testing is a challenge. Sometimes this is due to certification requirements that take time and money. Sometimes it is due to the potential negative impact that a test might have on normal operations. Whether the issues are regulatory, financial, or otherwise, researchers face a variety of challenging obstacles that restrict if not prevent forward movement. With new technology, I regularly hear practitioners say they are starved for results from real-world testing. Sharing this research with a broader audience may be the first step in creating applications useful to homeland security.

A NOTE ON SELECTING AND READING PAPERS

As is often the case when addressing the breadth of Homeland Security, this set of papers covers more ground than would be of interest to a single reader and the scientific nature of the work may go deeper than a reader would otherwise need to go. Nonetheless, it is worthwhile to periodically sample work of this nature and to consider the potential strategic impact this kind of work can have on the practice and policy of homeland security (see Table 1).

It is also worth noting that the papers present research in various stages of development. Some present technologies that have been tested in laboratory and limited real-world environments and could be on a track toward commercialization in the foreseeable future. Others are less far along, one being a concept that will be subject to its first field trial this spring. Each offers interesting insight into the world of science and technology that enables the strategy and policy options available to homeland security leaders.

OVERVIEW OF PAPERS

The 2010 IEEE HST Conference offered scientists and engineers four tracks from which best papers were selected. The tracks focused on the following areas:

1. Homeland Cyber Security
2. Attack and Disaster Preparation, Recovery and Response
3. Land and Maritime Border Security
4. Counter-Weapons of Mass Destruction Techniques and Critical Infrastructure and Key Resources Physical Security

In addition, the best-paper selection committee chose one paper as the conference best paper.

The sections that follow identify the best papers from each track and provide a non-technical overview of some of the ideas presented in each paper. This supplement to Homeland Security Affairs contains the full text of the papers as well.

COUNTER-WMD TECHNIQUES AND CRITICAL INFRASTRUCTURE AND KEY RESOURCE PHYSICAL SECURITY ASSUMPTIONS

The best paper in this track was "Gamma-Insensitive Fast Neutron Detector with Spectral Source Identification Potential" by Rico Chandra of Arktis Radiation Detectors Ltd, and Giovanna Davatz and Alexander Howard of Arktis Radiation Detectors Ltd, Zurich, Switzerland, and ETH Zurich's Institute for Particle Physics.

Detection and discrimination of possible nuclear threats is a major national security priority. The paper by Chandra, et. al. addresses two issues that are important in this area: (1) detecting nuclear materials even when heavily shielded or at a large standoff from the detector and (2) finding an alternative to currently used thermal nuclear detectors that require a type of helium that is in short supply (3He). In the process, the paper addresses scientific rationale for considering a type of technology that historically has been categorically dismissed

but that may be more effective than existing technology in achieving some homeland security objectives in the maritime environment, in land-border crossing, in cargo screening, and in other areas where importation of weapons of mass destruction is a concern.

The initial goal of this research was to design a neutron detection system that is more sensitive to weaker and shielded neutron sources than conventional thermal neutron detection systems involving moderators. This would address the need to detect nuclear radiation at lower levels including those that might be found when sources are well shielded. A secondary goal is to increase the feasibility of widespread deployment of advanced nuclear detection systems that are currently limited by the availability of 3He. This paper presents a fast neutron detector using 4He (the type of helium found in children's balloons) that addresses both issues. The system allows detection and identification of energetic neutrons as are emitted by nuclear materials, without confounding this signal with the strong natural background of predominantly low-energy neutrons. At the same time it reduces false positives; integrates with a high-performance, low-cost data acquisition system; and addresses the need for overall cost effectiveness.

The paper also points out a potential investment and resource allocation issue. Currently, fast neutron detection (the type of detection presented here) is not considered viable because it does not achieve as good an absolute efficiency rating as thermal neutron detectors. This means that this class of detectors (fast neutron) is not considered for security applications. However, the authors find that if you factor in the impact of background radiation, the fast neutron detector actually performs well, and has the potential to detect configurations of shielded nuclear material that may elude detection by conventional means. This suggests a change in the metric used to evaluate performance and a change in the strategy to better address shielded sources and other situations when there is a low level of radiation.

ATTACK AND DISASTER PREPARATION, RECOVERY, AND RESPONSE

The best paper in this track was "Leveraging Public Wireless Communication Infrastructures for UAV-Based Sensor Networks" by Kai Daniel and Christian Wietfeld, of Communication Networks Institute, TU Dortmund University.

Remote sensing by unmanned aerial vehicles and systems (UAV and UAS) has become an increasingly useful capability on the battlefield. Recent advances in related technologies mean that smaller, micro UAV are available at much lower cost to civilian agencies. In the latter context, UAS comprised of micro UAV paired with sensors and cameras have the potential to increase situational awareness by providing incident information to commanders on the ground.

Deployment of these systems depends, in part, on the ability to transmit navigation, control, and sensor information between the UAV and a mission control center in near real-time. However, limited frequency availability and the cost of proprietary communication technologies hamper deployment.

Daniel and Wietfeld propose a meshed network for airborne communication using widely available civil mobile communications systems to transmit navigation, control, and sensor information. This aerial "meshed network" has each aircraft (network node) also functioning as a relay for others. (Think of a cell phone network in which each phone could not only communicate with a cell phone tower, but could also relay calls from other nearby phones, potentially eliminating dead spots and extending the reach of cell phones to otherwise out-of-range towers; this would be a meshed network.) The vision put forth by Daniel and Wietfeld is for swarms of sensor-enabled micro UAV to be deployed into clouds or into areas that are otherwise not accessible, form an ad-hoc meshed network, and improve situational awareness. Field trials will begin next year.

HOMELAND CYBER SECURITY

The best paper in this track was "Prototyping Fusion Center Information Sharing;

Implementing Policy Reasoning Over Cross-Jurisdictional Data Transactions Occurring in a Decentralized Environment" by K. Krasnow Waterman and Samuel Wang of the Decentralized Information Group, CSAIL Massachusetts Institute of Technology.

Information sharing is widely viewed as essential to homeland security and mandated by Executive Order. However, the maze of laws and policy that governs what can be shared, with whom, under what circumstances, etc. is mind-bogglingly complex. The number of information sharing events that are contemplated every day compounds that complexity. The question is whether it is possible to automate the process, to quickly sort out the complexities governing sharing, and to evaluate whether a given information-sharing event is allowed.

The basic idea behind this technology is to make sure that we share information with the right people and organizations and do it in a manner that is consistent with policy. For example, if two people want to exchange a pdf, they shouldn't have to become legal scholars just to figure out whether they can exchange it.

Waterman and Wang propose and test a prototype of an "accountable system" for automating the process of evaluating information sharing events within the context of fusion centers. This system uses semantic web technologies, a class of technologies that attempt to understand the meaning of data and apply reasoning based on the meaning. The prototype also has what they call "policy awareness" so it knows which policies apply to which data.

For example, if the data indicates a health record contains personally identifiable information, and the policy says personally identifiable information cannot be shared with the requesting agency, then the system must be able to figure out that the health record data cannot be shared and why – this is reasoning based on meaning since the system was never programmed to disallow sharing the health record. Of course the reasoning, like the laws and policy, needs to be able to address more complex relationships.

To illustrate, the authors provide the following example from Massachusetts law: "Information shall be provided or made available… only if the individual named in the request or summary has been convicted of a crime punishable by imprisonment for a term of five years or more, or has been convicted of any crime and sentenced to any term of imprisonment, and at the time of the request: is serving a sentence of probation or incarceration, or is under the custody of the parole board…."

Constructing a system that could do this required that the researchers design and develop several different elements. They had to develop a way to represent laws and policies that a computer system could understand. They also needed a representation of the data that might be shared – in a way that could transcend the nomenclature used by different agencies in a fusion center – and could be "reasoned over." Next, they needed to build a "reasoner" that would apply the laws and policies to the underlying data (including supplemental data provided by the user at the time a request for information is made) and provide the justification for why the event is or is not compliant. Finally, they needed a user interface that would present the justification in a way users would understand.

The paper explains the underlying technologies (e.g., semantic web, accountable systems), the modeling of rules and data, and other details of the prototype system. Numerous examples illustrate how such a system can work. Results of a successful test of the prototype demonstrate the feasibility of using this type of system to perform reasoning based on complex laws.

Other uses of the system include: retrospective application of new policy to test the impact of the new policy on information sharing, running hypothetical transactions against many policies, and profiling usage of existing policies (including gathering data on exceptions, etc.).

LAND AND MARITIME BORDER SECURITY

The best paper in this track was "Intelligent Acoustic and Vibration Recognition/Alert Systems for Security Breaching Detection, Close Proximity Danger Identification, and Perimeter Protection" by Alireza A Dibazar, Ali Yousefi, Hyung O Park, Bing Lu, Sageev George, Theodore W Berger, Department of Biomedical Engineering, University of Southern California.

Protecting our borders from intrusion is a critical element of homeland security policy with significant sums invested in people and systems to prevent unauthorized entry.

There are a variety of competing detection and alerting technologies to aid in this effort. These include video (good in long-range, unobstructed view environments), and aboveground motion sensing technologies (good where normal movement in the environment can be addressed).

Another approach to protecting borders is to deploy sensors at locations where foot and vehicle traffic are likely to create sound and vibration. An important challenge is to identify those sounds and vibrations that represent a potential threat while ignoring those that are benign. It would be useful, for example, if a system could tell the difference between a person climbing a fence and an animal bumping into the fence, or a fence rattling in the wind.

Dibazar et. al. present results of their work on acoustic and vibration recognition and alerting systems. Their laboratory and field tests indicate it is possible to identify the type of motor vehicles approaching a sensor, the presence of pedestrians, and climbing, kicking, or rattling of fences. They also present information about the low rate of false positives in both controlled and field experiments.

Using various technologies (video, aboveground motion sensing, acoustic, and vibration recognition systems in combination) and matching the technology to the environment makes for a sensible, multilayered approach to border security.

In addition to international border protection, potential applications of this technology include airport perimeters and other critical infrastructure facilities with significant exposure to intentional fence breaches.

CONFERENCE BEST PAPER

The best paper in this track was "Augmenting the DGPS Broadcast with Emergency Information – Potential Coverage and Data Rate" by Richard J. Hartnett, U.S. Coast Guard Academy, Peter F. Swaszek, University of Rhode Island, and Keith C. Gross, U.S. Coast Guard Academy.

Emergency messaging is a critical component of response and recovery communication strategies. Finding efficient ways to reach people within a specified geographic area is a central concern. Radio transmissions are one way to achieve this goal. However, frequency availability, transmission tower location, and other factors affect the ability to use radio transmissions. One possible approach to this problem is to broadcast text messaging using existing transmitters, provided the operational impact on the transmitters' primary function is acceptable.

Hartnett et. al. present results of research and evaluation of a technique they developed for adding emergency messaging to the differential GPS broadcasting system run by the U.S. Coast Guard. Since the system and transmission towers already exist and the system currently blankets most of the continental U.S. (CONUS) and the entire U.S. coastline, the question is whether it is possible to add emergency messaging to transmissions without impacting the operational mission of the existing system. If effective, this approach would address some of the limitations present in cellular network SMS messaging systems.

The authors develop and evaluate an approach to adding this messaging, called "phase trellis overlay." They have tested to determine that the current antennas can transmit the modified signal and that receivers can be built to decode the signal. The challenge presented in this paper is to optimize the approach to provide desired coverage and data transmission capability

while minimizing impact on legacy (existing) receivers.

Successful testing and implementation of this approach holds the potential to provide emergency data communications as well as geo-location and other benefits for emergency personnel during a disaster. Critical next steps include testing this CONUS-wide to understand coverage across the country.

(It is this paper's reference to the search for alpha that inspired the title of this introductory article: "Policy, Practice, and the Search for Alpha.")

CONCLUSIONS

We are pleased to present this set of best papers from the IEEE's HST conference as a way to provide exposure to leading edge research and to encourage collaboration among policy makers, practitioners, scientists, and engineers.

Table 1: Strategic Impact of HST Conference Papers

Paper	Prepare and Prevent	Respond and Recover	Anomaly Detection	Interoperability and Communication	Information Sharing and Collaboration	Situational Awareness
Gamma-Insensitive Fast Neutron Detector	X	X	X			X
Using Public Network Infrastructures for UAV Remote Sensing		X		X	X	X
Prototyping Fusion Center Information Sharing	X	X		X	X	X
Intelligent Recognition of Acoustic and Vibration Threats Protection	X		X			X
Augmenting the DGPS Broadcast with Emergency Information		X		X	X	X

ABOUT THE AUTHOR

***Robert Josefek** is an expert in information and decision sciences including social media, social networking, and knowledge management. He works with public and private sector organizations to help executives and senior managers understand strategic and organizational issues relevant to their information technology options, improve planning and investment decisions, and establish organizational design and development strategies to prepare for future advances. Dr. Josefek is an adjunct professor at the Naval Postgraduate School's Center for Homeland Defense and Security, served on the faculty at the University of Southern California (USC) Marshall School of Business, taught at the University of Minnesota, and is a member of the Homeland Security Affairs Review Board.*

ACKNOWLEDGEMENTS

I would like to thank paper authors, presenters, session participants and committee members, including Rob Cunningham and Jerry Larocque of MIT Lincoln Laboratory, who contributed to ideas presented in this article.

IEEE and HST Background

The Conference on Homeland Securities Technology is an Institute of Electrical and Electronic Engineers conference. The Institute of Electrical and Electronic Engineers (IEEE) is the world's largest professional association for the advancement of technology. It traces its roots back over 125 years and has a worldwide membership of about 400,000.

HST Conference Background

The tenth annual Conference on Homeland Securities (HST) was held November 8-10, 2010 with about 400 registrants, from public, private, and academic institutions engaged in research, development, and manufacture of homeland security technologies. In addition to papers presented during track sessions, keynote speakers addressed plenary sessions. Poster sessions and tutorials rounded out the conference.

In the months leading up to the conference, papers submitted to each track go through a peer review and selection process. The next HST conference will be held in the Boston MA area, November 15-17, 2011 (see http://www.ieee-hst.org/).

Best Paper Selection Process

Each track chair or committee nominated two papers. A best paper selection committee then reviewed and chose the four best-in-track papers and the conference best paper.