Homeland Security
Science and Technology

Homeland Security Science and Technology Advisory Committee (HSSTAC): Quadrennial Homeland Security Review Subcommittee

Chemical, Biological, Radiological, and Nuclear Detection White Paper

March 10, 2017

This publication is presented on behalf of the Homeland Security Science and Technology Advisory Committee, Quadrennial Homeland Security Review Subcommittee, Chemical, Biological, Radiological, and Nuclear Detection, chaired by Eric Haseltine with contributions from Dr. Gerald Parker, Dr. Yacov Haimes, Mr. Daniel Dubno as part of recommendations to the Department of Homeland Security, Under Secretary for Science and Technology, Robert Griffin (*Acting*).

<Signature on File>

Eric Haseltine
President
Haseltine Partners, L.L.C.

HSSTAC Staff: Michel Kareis, HSSTAC Executive Director/DFO and Gretchen Cullenberg, QHSR Subcommittee support.

Homeland Security
Science and Technology

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR DETECTION AND HOMELAND SECURITY

Dr. Eric C. Haseltine, Subcommittee Chair; Dr. James Decker, Dr. Marian Greenspan, Mr. Philip Coyle, Dr. Michael Goldblatt, Dr. Kathie Olsen, Dr. Gerald Parker

White Paper for HSSTAC Quadrennial Homeland Security Review (QHSR) Subcommittee in support of the 2018 QHSR

Digital "ripples" from connected devices can help detect and manage CBRN events

Introduction

There is room for improvement in our ability to detect, locate and identify chemical, biological, radiological and nuclear defense (CBRN) events in the Homeland, and to differentiate such willful events from "natural" occurrences such as infectious disease outbreaks or hazardous materials (HAZMAT) releases. Further, to contain the damage from CBRN terrorism, it would be desirable to identify everyone that a CBRN event has affected, along with where those affected individuals subsequently go.

The opportunity

Digital devices connected to the global network are rapidly finding their way into almost every facet of life. In addition to computers, smart phones, tablets, game consoles, new categories of connected devices such as fitness wearables, digital fashion accessories, Internet of Things (IOT) appliances, security systems, self-driving cars, robotics, smart toys, industrial control and home automation systems are coming on the market at an accelerating pace. Over the next decade, these connected devices and others, such as Augmented Reality systems and telemedicine sensors will continue to penetrate new niches. All of these connected devices have sensors of one kind or another (e.g. accelerometers, GPS, RF sensors, cameras & microphones) so that it will be theoretically possible to "instrument" virtually the entire population of the U.S. in one form or another, and to use this synoptic instrumentation to swiftly detect and respond to CBRN events.

One way to think about this opportunity is to view the data flows created by interconnected devices as rivers of bits that feed an immense ocean of bits containing vast, up-to-the-moment information about the human condition. Events that cause social disruption leave ripples and wakes in this digital ocean. And, just, as different kinds of vessels produce different kinds of wakes, different kinds of social disruptions produce unique digital signatures that can help identify the nature of the disruption, along with its time and place. In some cases, sophisticated analysis can also pinpoint who *caused* the disruption. Finally, most promising of all are opportunities to detect “bow waves” of disruption that *precede* a CBRN event, so that the event might be prevented from occurring in the first place.

Maintaining both the appearance and fact of privacy while collecting and acting on streaming data from billions of connected sensors in our population, will be essential to realizing this vision. Fortunately, innovative approaches to preserving privacy—such as machine learning applied to pooled, anonymized data, are fast emerging to address this challenge.

Accordingly, all the proposed approaches that follow assume that privacy must be protected, and *will* be protected using these emerging techniques.

Candidate approaches

A multi-billion-dollar industry has already emerged to detect and act upon digital “wakes” and “bow waves.” For example:

- A contractor to the NFL has analyzed localized Twitter feeds to detect fights in stadiums during games *before* stadium operators themselves knew of the fights.
- A financial technology (Fintech) company has analyzed pooled, anonymized data from cell operators (including GPS and other location data) to predict moves in equities and commodities markets based on changes in the movements and pattern of life of workers in financial districts.
- Health officials in Africa have used similar data to identify sources and vectors for spread of Dengue fever and Ebola.
- Georgetown University has detected flu outbreaks in Asia weeks ahead of the World Health Organization by scraping and analyzing digital and social media.
- Foreign Policy analysts can sometimes predict and localize political demonstrations from the volume and location of mobile text and social media posts (purchased in anonymized form).
- Mobile apps can combine sensor feeds from many handsets to create vast “synthetic apertures” to detect earthquakes (from accelerometer data), explosions (from microphones) and even gamma radiation (from activation of cell cameras).

<u>Detecting CBRN events</u>

These kinds of techniques can be adapted to detecting CBRN events as follows:

- Changes in pattern of life manifested in GPS movement and accelerometer movement in mobile and wearable devices
    - Rapid movement away from (or towards) a location.
    - Sudden loss of connectivity to multiple mobile devices in a location.
    - Changes, over time, of accelerometer data indicating reduced physical activity or slowed physical activity due to illness or impairment. Changes in data from fitness wearables measuring heart rate, number of steps and other physiological signals.

- Analysis of content of social media posts, and traffic analysis of anonymized, but localized messaging to identify location and nature of CBRN event.
- Sensor activity from cameras, microphones, accelerometers in mobile devices, laptops, computers and IOT devices (home security/automation, municipal, industrial) can detect, localize and sometimes identify CBRN events, including those producing ionizing radiation.
- Techniques for analyzing such data (that are beyond the scope of this document) can sometimes identify who had prior knowledge of a CBRN event and even predict an event before it occurs.
- Machine learning technology can sometimes, based on analysis of historical events, differentiate between natural (e.g. disease/HAZMAT) and intentional acts.
- Spikes in internet search volume for keywords describing an event (such as explosion) can be detected minutes after the event.
- IOT smoke detectors can be easily modified to detect localized increases in ionizing radiation (detecting radiological events and possibly the presence of fissionable material *before* the material detonates).

Managing CBRN events

- Mobile GPS data (and cell/sector handshaking data) can identify handsets that were exposed to pathogens, toxins and radioactive material so that (with suitable civil liberties protections) affected individuals (and people the individuals later meet) can be found and treated.
- Personalized, localized text messaging to mobile devices can instruct affected individuals (detected as just described) to seek help, avoid spreading toxins or disease or where to seek shelter or protection from a recent or imminent event in specific locations.
- Connected sensors can localize events so that first responders know where to go.
- Emotional sentiment analysis, examining content of electronic messages and posts, can indicate level of panic and effectiveness of government emergency messaging.
- Digital "bow waves" and "wakes" can sometimes pinpoint who caused a CBRN event so that law enforcement and security officials can "find, fix and finish" the perpetrators.

Recommended next steps for DHS

There are many technical challenges to collecting, analyzing and acting upon digital "bow waves" and "wakes." But early work in commercial sector suggests that these challenges can and will be surmounted, and that DHS can take advantage of these rapid advances through a multi-step process as follows:

Engage data scientists in DHS S&T and other stakeholders at DHS to:

- Prioritize gaps in detection, identification, localization and attribution of CBRN events.
- Survey leading ongoing efforts and players in the private sector that can bridge these gaps.
- Identify the most promising near-term applications.

- Begin pilot programs.
- Look for ways to exploit these new technologies for other pressing DHS needs such as border protection, counter-terrorism and natural disaster management.
- Look for ways to integrate “digital ocean” sensing and analytics with existing DHS sensors and analytics.

As important as these S&T efforts will be, they pale in importance to the daunting policy challenges associated with collecting, analyzing and acting upon disturbances in the digital “ocean.”

Accordingly, in parallel with the S&T initiatives, DHS should Identify & develop approaches for sensitive policy issues, including:

- Privacy.
- Meta-data standards for “connecting dots” among diverse digital devices data streams and cloud storage sources.
- Access to private data (e.g. cell carriers, ISPs).
- Mandates for mobile device emergency modes and applications (e.g. radiation detection, exploitation of other sensors from native Apps in all handsets).
- Mandates for new features in networked IOT devices (e.g. detecting and reporting increases in ionizing radiation in smoke detectors).
- Public messaging and education to convince the population both of the need for such measures and that privacy can and will be protected.
- How to take advantage of classified data and techniques to augment unclassified initiatives, without compromising national security.