Testimony of Honorable Reginald Brothers

Principal

The Chertoff Group

U.S. House of Representatives

Committee on Homeland Security

Subcommittee on Emergency Preparedness, Response and Communications

November 7, 2017

Good morning Chairman Donovan, Ranking Member Payne, and distinguished members of the Committee. Thank you for the opportunity to testify before you today on the role and effectiveness of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T). S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise (HSE). Technology simultaneously enables both homeland security operators and malevolent actors and, as a result, has a significant and expanding impact on current and future threat environments. Having served in both the Departments of Defense and Homeland Security in senior leadership positions in science and technology, I'd like to start by giving my thoughts on the current and future threat environment as a way of providing context for the work of S&T.

We are now in a post-industrial age, with a global interconnected web leading to a highly integrated world with supply chains that reach thousands of miles. Things that previously were done only by nation-states are now accomplishable by sub-state actors, gangs, groups and even individuals.

For the period of the Cold War, it was possible to develop strategic nuclear weapons, stealth platforms and precision weaponry and retain a competitive advantage for a decade or more. However, with the hyper-connectedness of our world and the subsequent democratization of technology, it no longer possible to develop technology based capabilities for national security that have any significant temporal advantage. The power to inflict harm is no longer based solely with nation states. Our new reality is an asymmetric threat environment where individuals attack government institutions and nation states attack civilian infrastructures with little fear of retaliation or even attribution. With easily accessible technologies such as cyber tools, drones and potentially bio-weapons, it is possible for individuals to cause significant financial and physical damage as well as endanger human life. While we are used to discussions of precision targeting of kinetic weapons, we are now discussing precision targeting of

individuals and content on Facebook. And technology continues to accelerate with artificial intelligence, the Internet of Things, commercial drones and satellite constellations, synthetic biology, blockchain and quantum computing all promising tremendous benefits to society but with also the potential to create devastating threat vectors and complex and vulnerable threat surfaces.

What this context tells us is that the nation needs a sufficiently and consistently funded, agile, adaptive, relevant and rapid innovation engine to confront the current and future threats to our national security. DHS S&T has worked hard to focus on being highly relevant -- shifting from the past focus on long-term basic research to near-term operational impact. I think S&T is now an important asset for the Secretary as one of the few cross-Departmental entities. I'd like to now provide a few examples.

DHS S&T created the Data Analytics Engine (DA-E) which is a Department-wide resource for leading edge data analytic and machine learning technologies applied to Homeland Security mission sets. A laboratory has been developed where operational personnel can work with S&T staff to evaluate and co-develop technological solutions. Using this capability S&T helped NPPD deploy a social media capability to monitor publicly available posts regarding critical infrastructure and public health. S&T delivered over 370 requests for help to emergency responders. The S&T DA-E provided solutions using advanced facial recognition tools that identified 475 child sex trafficking victims, leading to their rescue from abusers.

At the direct request of the NYPD, conducted further experiments in identifying and characterizing live streaming social media sources that are affiliated with terrorist or other criminal activity. In addition, outside of New York, S&T will evaluate an even more extensive selection of social media analytical tools on behalf of I&A, CIS, and CBP for screening and vetting to detect, characterize, and locate source(s) of content of interest on social media platforms like Periscope and Facebook Live.

In partnership with the New York Police Department and Metropolitan Transportation Authority (MTA), S&T installed a 'permanent' testbed in New York City's Grand Central Terminal, an extension of S&T's pilot demonstrations successfully measuring and mapping how and where a bioagent would be transported in the event of a terrorist attack in the subway system.

On behalf of TSA, S&T conducted three live-fire exercises to better understand Home Made Explosives (HME) capabilities and impacts on critical infrastructure.

S&T completed the SkyNet Field Experiment, a Tucson Border Security Operational Exercise for CBP and ICE to evaluate border security technology capabilities linking Border Patrol, HIS and industry. This field exercise will be used to further develop and deploy tactical data and video from Border Patrol sensors and Small UAS platforms. S&T developed sensors for Field Agents at the Tactical Operations Center, the Border Patrol eGIS system, and remote locations such as the Air Marine Operations Center. The FE was a series of scenarios centered on illegal entry by walkers, vehicles, and air platforms such as ULAs (Ultra Light Aircraft) in a Southern Border environment.

S&T finalized the standup of the Common DHS UAS Test Site for use by S&T, FEMA, Coast Guard, CBP, and Secret Service for testing and training on UAS technologies. Unlike the counter UAS program this test site will allow for development of UAS technologies by DHS operational components. In addition, S&T will finalize counter UAS agreements with DOD to consolidate all UAS threat databases and libraries under the JIDO umbrella.

S&T deployed the Counter Small Unmanned Aerial System (C-UAS) Advisory and Review Toolkit (C-SMART) to the Secret Service. C-SMART is a suite of computer models, databases, and analysis tools to analyze and plan C-UAS security postures for specific operations – this capability has helped Homeland Security Enterprise (HSE) partners understand the C-UAS threat, and optimize security posture plans. C-SMART has been used in direct support of National Special Security (NSSE) and Special Event Assessment Rating (SEAR) identified events, such as the Inauguration and the Super Bowl.

S&T deployed the Next Generation Incident Command Center (NICS) to even more emergency operational centers across the nation and world. NICS is a web-based communication platform that enables responders on scene to share data and information using open standards, and request and receive assistance from remote experts in real-time. Developed in collaboration with MIT Lincoln Labs and the Coast Guard, S&T's NICS is in use by Coast Guard assets, Cal Fire, California OES, State of Victoria Australia, and NATO member and partner countries as part of NATO's Science for Peace and Security Project Advanced Regional Civil Emergency Coordination Pilot. S&T received funding from Australia and NATO for further development of this platform. S&T has made NICS available on GitHub, the world's leading software development platform.

S&T transitioned the National Hurricane Program Technology Modernization HURREVAC-eXtended (HVX) to FEMA. HVX enables emergency managers to visualize hurricane risks associated with their specific evacuation zones, resulting in reliable and better-informed evacuation decisions. Two major improvements for HVX include providing a web-enabled system to make training widely available to emergency managers online, as well as accessible

via mobile phone—a FEMA requirement. The initial HVX Beta will complete its transition in May 2017. Once fully operational at FEMA in 2018, substantial savings are expected by avoiding unnecessary "over" evacuations and saving lives by preventing "under" evacuations. HVX makes it possible for web based training allowing FEMA to train hundreds of thousands of emergency managers compared to less than 100 per year with the previous system, greatly reducing training costs and making it possible for greater numbers of emergency managers to gain critical skills in evacuation decision making.

S&T developed the First Responder Jamming Exercise. The focus of the work are the technical and operational challenges of commercially available jamming technologies on first responder communications. This work done with NPPD, FEMA, Coast Guard, Los Angeles, Houston, Arizona, NYPD among others, and brings industry to the field to work through this growing threat. S&T and OGC have sixteen limited purpose Cooperative Research and Development Agreements (CRADA) in place to test equipment. From last year's exercise S&T was able to develop a training module with FLETC which was used at the inauguration to train first responders to identify and mitigate use of jamming technologies.

S&T also provided support to the response and recovery efforts from Hurricanes Irma and Harvey:

- As of Sept 12, 9 S&T surge capacity volunteers had been deployed. A system the S&T First Responders Group (FRG) and NPPD collaborated on is preparing reports on the number of businesses open and progress of business restoration. Information from the reports is being shared to emergency managers and others.
- FRG has provided approximately $76K in communications equipment to emergency managers in Georgia to support Irma recovery. As of 11 September, the Program Manager, Shawn McDonald, the Irma ATAK server is in full deployment more than a hundred organizational users.
    - S&T is providing the Android Team Awareness Kit (ATAK) technology and training to DHS components and responders Supporting Hurricanes Irma that allows them to see where and collaborate with responders and support personnel in real-time as well as to plan and track multiple locations where support/response is needed.
- S& T has used a software program to develop aerial and satellite photos that maps high risk structures in Florida, Georgia and South Carolina to allow for better response and recovery and made these photos available to FEMA and search and rescue teams as well.
    - Flood APEX Map data sets have been completed for Georgia and South Carolina as well as Florida, in support of Irma. Flood apex has worked with ORNL to put

together building outlines datasets from high resolution satellite imagery for the Ga and SC coastal counties. Previously completed initial map data sets of building structure outlines for Puerto Rico, the Virgin Islands, and south Florida and assisted FEMA with publishing those data to the web for broad community access as well as distribution to search and rescue and volunteer teams.

- S&T FRG is providing additional access to the HVX prototype system, which allows emergency managers, FEMA response officials and others to make timely and accurate evacuation related decisions more efficiently.
    - 200+ FEMA, State and Local users have been given access to HVX Prototype
    - U.S. Army Corps of Engineers is a HVX user
- S&T is providing a social media monitoring tool and training to allow NPPD analysts real-time updates on threats and issues including health issues, people requesting medical assistance or rescue, status of utilities and resources, and more, to allow better allocation of resources and response.
- The S&T funded storm surge software (ADCIRC) provides emergency managers early and accurate predictions about storm surge and coastal flooding to allow them be make better decisions on evacuations, positioning of resources and other response and recovery issues.
    - RADM Peter Brown is using the ADCIRC results to plan for evacuation of USCG staff from Key West USCG housing. On September 6, told Dr. Rick Leuttich, CRC leader, “The [ADCIRC] model was key to my decision regarding aircraft protection in Puerto Rico and our COOP decision for Miami. I’ll be watching it with every update.”
- The DHS S&T Coastal Resilience Center of Excellence (CRC) worked closely with the Texas State Operations Center and NOAA to provide modeling and storm surge predictions to better enable prepositioning of resources, evacuations and recovery. The CRC ADvanced CIRCulation (ADCIRC) storm surge/coastal flooding modeling team is providing models for Texas/Gulf of Mexico. DA-E social media analysis tools: S& T’s HSARPA Data Analytics Engine (DA-E) continues generating reports from open source and social media data. The tool, requested by NPPD, monitors social media for emergent threats and augments situational awareness regarding public health and critical infrastructure. It provides automated, real-time monitoring of social media data related to public health, communications, dams, electricity, oil & natural gas and water. Urgent requests for help (e.g., infant not breathing) were forwarded to FEMA’s National Watch Center. Updated reports and documents were provided approximately every 3 hours to NPPD. As of August 28th, nearly 4,000 posts had been collected and analyzed to identify approximately 250 of the most relevant. DA-E also established a new collection effort on August 28th to identify an additional 100+ posts specifically

focused on calls for help and will be sending these posts to FEMA. The DA-E team continues to analyze information related to infrastructure protection interests and producing regular reports. HSARPA DA-E has initiated transition of technical capabilities for situation awareness regarding critical infrastructure using open source and social media data to NPPD.

Silicon Valley Innovation Program

Starting in December 2015, DHS S&T initiated the Silicon Valley Innovation Program as an effort to engage creative scientists, engineers and technologists from across the world in solving pressing problems in National Security. As of the present time, an awareness has been built with more than 1000 start-ups accelerators and venture capitalists. Six topic calls have been published: IoT Security, K9 Wearables, sUAS Capabilities, Enhancements to the Global Travel Assessments System (GTAS), and Enhancing CBP, Airport Passenger Processing, Financial Services Cyber Security Active Defense (FSCSAD). 116 Phase I and 5 Phase II applications have been received. Applicants have been from across the country and international. There have been 9 Phase I awards and 4 Phase II awards to date.

Collaborations

For operational relevance, collaboration with users and industry is essential. The DHS S&T Cyber Security Division has developed specific and relevant collaborations with the Energy, Financial and Automotive sectors:

- Energy sector
    - Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) is an ongoing collaboration of oil and natural gas companies and DHS S&T.
        - LOGIIC facilitates cooperative research, development, testing, and evaluation procedures to improve cyber security in petroleum industry digital control systems.
- Financial sector
    - The Next Generation Cyber Infrastructure (NGCI) Apex program will identify, test, evaluate and deploy cutting-edge technologies to deter cyberattacks against the financial sector. The program will concentrate on delivering capabilities identified by the financial sector to address five primary functional gaps
    - Stakeholders: U.S. Department of the Treasury, the Financial Services Sector, the OTA Contractor and private technology vendors.
- Automotive Sector

- The (Cyber Physical Systems Security) CPSSEC program focuses include working collaboratively with automakers and leading researchers to increase vehicle cybersecurity, funding research projects to enhance auto cybersecurity, and helping to upgrade the federal government's fleet of automobiles.

With the successes discussed above, it is clear that DHS S&T is working towards being the agile, adaptive and rapid innovation engine I described. That said, there is a second context to consider when evaluating the potential of S&T to be effective.

That second context is the breadth and depth of its mission and the level of appropriated funds. The S&T Budget for DoD for FY18 is approximately $14B while that of DHS S&T is approximately $600M. DoD has a significant national laboratory infrastructure for evolutionary capability improvements and the Defense Advanced Research Project Agency funded at approximately $3B for revolutionary/disruptive improvements. In contrast S&T is asked to provide all R&D across both evolutionary and revolutionary domains with less than an order of magnitude of funding. While there is some cross-pollination possible between the Departments, in many cases mission specificity and affordability factors limit the ability of DHS components to procure and sustain DoD technologies. As such, I believe that S&T is underfunded for its stated responsibilities across all of the DHS mission sets.

In fact, if the FY18 budget cuts remain in effect there will be severe impacts to S&T ability to do its job. For example, these budget cuts will reduce the funding of the Cyber Security Division by 20% and the Chemical Biological Division by approximately 60%.

Cyber security is a challenge that is exponentially increasing with time. Observed malware has increased 40 times in the past ten years. Observed attacks on Critical Infrastructure have increased 1.5 times in just the past three years. With the emergence of the Internet of Things, Autonomous vehicles and other networked innovations, the threat surfaces of our national security are rapidly expanding.

While awareness of the need for Cyber Security is increasing, the same is not necessarily true for Chemical and Biological security.

Threats from chemical and biological threat agents—known and yet unknown synthetic variations—are real, growing in potential and consequence, and becoming more attractive to terrorist organizations. As law enforcement organizations around the world make it more difficult to acquire materials to make explosives and gain access to quantities of firearms, chemical agents and eventually, biological agents will become the terror weapons of choice.

Recently, researchers at the University of Alberta announced the artificial synthesis of Horse Pox, a close "relative" of Small Pox. A number of prestigious scientific journals have refused to publish the details of this accomplishment for fear that if a step-by-step procedure were to

become available, those with skills in this technology could easily produce the human Small Pox virus and unleash this terror on an unsuspecting world population.

After the attacks of 9/11, the U. S. government recognized that defensive measures had to be implemented and maintained to protect civilians from these methods of terror attack. To this end, Congress and President Bush created a dedicated organization and facilities within the Department of Homeland Security to work closely with law enforcement and the intelligence community to identify growing threats, develop technologies to detect threats and support first responders if the unthinkable ever happened. In addition to establishing a specialized federal and contractor workforce in chemical and biological defense technology development, two unique facilities, the National Biodefense Analysis & Countermeasures Center (NBACC) and Chemical Security Analysis Center (CSAC) were approved and funded by Congress. Each of these facilities is recognized within the U. S. as the nation's focal points for biological and chemical defense awareness and response. These centers not only support many domestic government agencies at the federal, state and local levels but also work closely with international partners in thwarting potential terrorists from using chemical and biological warfare agents. There is widespread agreement that the DHS capabilities in chemical and biological defense science and technology are unique and needed to provide a foundation for this critical area of national security. But the funding for these centers is being cut due the FY18 budget pressures.

Given the threats to national security that our current global context mandates, I am very concerned about the impact of the FY18 budget cuts. From my personal experience I know that one of the most disruptive forces for a technologist and an innovation organization is uncertain and unstable funding. This challenge is magnified at DHS, because the threat environment can change on a frequent basis which can call for rapid change of investment across the R&D portfolio to meet the immediate threat. However, while I am concerned, I also believe with the appropriate support from the Department and Congress, S&T can meet the challenges of the 21st Century.