Elisha Hubbard
LEPSL 530: Public Safety Law
University of San Diego: Professional and Continuing Education

MEMORANDUM FOR: Sheriff

SUBJECT: Combating Terrorism through Alternative Platforms

Crime and terrorism being committed through or facilitated by the internet is not the next big thing, it is THE thing. It is not just targeting big government, IT IS HERE, and they were attempting to poison US. We must educate all of our Deputies in matters of terrorism and cybercrime so we can dominate on this field.

The Police Executive Research Forum (PERF), identified “Promising Practices” that we should initiate here in our department.

1) Develop a Strong Community Education Program (Crime Prevention Tasking)

Figures from cybercrimes and cyberterrorism are primarily unreported. Unreported activities do not get attention, do not get resources, and do not get legislature penalizing the crimes. Community education and community involvement must be a big ticket item. We must get the community involved. They must be able to recognize suspicious activity and crime, know how to report the activity, and demand stronger law enforcement action.

a) Educate the public via Public Service Announcements (PSAs) on TV, radio, social media, billboards, and community meetings. What is suspicious, what is a crime, how to recognize it, and how to report it.

b) Make the public aware of true threats. Keeping our citizens in the dark maintains an attitude of disconnectedness, naivety, and complacency that we cannot afford if we want the public to proactively contribute to the solution.

2. Obtain legislative backing to require reporting and stiffer penalties.

a) Mandate Reporting of Cybercrime and Cyberterrorism. Private companies must begin reporting true numbers so government agencies can get a proper account of monetary loss, numbers of victims, and cyberattacks or attempts. Online companies must be obligated to share information necessary to investigate online crime and terrorism.

b) Accurately high numbers will be the quantitative support necessary to get the attention of both the public and law makers to understand the significance of this criminal platform which will justify allotment of resources, prosecution, and stiffer penalties.

c) Instances of cybercrime and cyberterrorism are general intent crimes and we must stop looking at them by the impact of the single victim that reported the crime. These criminals are affecting multiple people on a massive scale. They just aren't getting caught. If a single crook stole the magical number of $950 from a hundred people in support of his criminal enterprise or terrorist cell, but only a few people reported the incident, are we really only going to hold this person accountable for a couple of misdemeanors? This is irresponsible law enforcement.

3. Task Forces

Cybercrimes and terrorism are primarily committed by crossing jurisdictional, state, even international boundaries. Here in San Diego County, we are fortunate to already have four task forces in place: Computer and Technology Crime High-Tech Response Team (CATCH), Regional Fraud Task Force (RFTF), Internet Crimes Against Children (ICAC), and the Regional Computer Forensics Lab (RCFL). As an agency, we must strengthen our independent investigative abilities so we can present a finer product to these tasks forces who can then assist to fill in the gaps, facilitate apprehension and enforce Federal prosecution.

4. Train and Establish a Cyber-Investigations Unit

a) Partnerships With Local Universities. Work with schools to host Computer Science Forensic degrees, training, and internships.

b) Identify current members of law enforcement who are technically savvy and make a direct effort train them in Counter-Terrorism and Cyber-Investigations and recruit technically savvy individuals as Cyber-Analysts. Different from Data, Cyber-Analysts, can proactively scour the internet, particularly social media sites, to identify Cyber-Terrorism sites, leaders, propaganda, and intelligence.

5. Identify and Monitor Methods of Non-digital Criminal and Terrorist Communications

As discovered in our recent terrorism case, there are sophisticated organizations who actively practice living off the grid and leaving no digital fingerprint. These methods, such as ham radios, are not only effective, but extremely reliable as they would still operate in the event of a power outage or natural disaster that disrupted services. Ham radio operation is a technology that has fallen to hobbyists. Prior to this case, there was never even consideration, at least at our local level, that ham radios were used as a method of criminal and terrorist communications.

Had it not been for my and Sharon Smith's combined experience in both terrorist activity and ham radio equipment and operations, the clues of this case would likely have been completely lost on a patrol officer and no further action would have been taken. It is a suggestion that these two subjects be presented in the next cycle of agency wide Continued Professional Training (CPT).

Elisha Hubbard

Elisha M Hubbard
Deputy Sheriff
San Diego Sheriff's Department

Resources:

Cilluffo, Frank. Homeland Security Policy Institute. "Counter Use of the Internet for Terrorist Purposes." May 24, 2013.

Police Executive Research Forum (PERF). "Critical Issues in Policing Series: The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime." April 2014.

Shetret, Liat. Center on Global Counterterrorism Cooperation. "Use of the Internet for Counter-Terrorist Purposes." February 2011.