B17 Connecting Digital and Physical Crime Scenes Using Cyber-Physical Crime Assessment

Richard D. Walter, MA, 1879 Chenango St, Montrose, PA 18801; and Peter R. Stephenson, PhD*, Norwich Univ, 158 Harmon Dr, Rm 205, Dewey Hall, Northfield, VT 05663*

After attending this presentation attendees will be introduced to a novel method of conducting an investigation where there are both digital and physical data to consider. Typically investigators seize computing devices (e.g., desktop computers, laptops, smart phones, tablets, etc.) and submit them to a digital forensics laboratory for analysis. Digital forensic examiners perform tests on the devices using digital forensic tools to extract typical data and through iterative communications with investigators search for individual pieces of data of possible interest in solving the crime.

This presentation will impact the forensic science community by demonstrating how Cyber-Physical Crime Assessment (CPCA) shows promise as a method for conducting a holistic investigation of a hybrid crime (a crime with both digital and physical elements). CPCA connects the physical and digital crime scenes together as a single crime scene, each with its unique characteristics, but intended to be viewed and analyzed as an integrated whole in much the same manner as a crime scene investigator would analyze the physical scene alone.

CPCA holds promise as a methodology for conducting a holistic investigation of a hybrid crime, defining hybrid as one with both digital and physical elements.

CPCA applies physical crime/crime scene assessment techniques developed over three decades and is based upon informal analysis of over 20,000 cases of violent crime. The presenters have ported these techniques into the digital world and refined them to include both digital and physical crime scenes where a single, hybrid crime has been committed.

This type of crime assessment consists of three aspects: description of the crime/crime scene using one or more of four sub-types, matching the sub-type(s) of suspects to the sub-type(s) of the crime, and analysis of the pre- and post-crime activities of key suspects.

Temporal analysis of pre- and post-crime activities, for example, is straightforward on a computing device due to the timelines that can be constructed using such things as file metadata and machine activity (e.g., When was the computer turned on or off? What cell phone activity can be matched to the pre- and post-crime activity? How does cell tower access compare with timelines of the physical event?) By considering the physical and digital aspects of the crime as a single crime scene with an integrated clue set, these connections become more obvious and useful in solving the crime, guiding digital forensic analysis, and supporting the solution for a conviction.

The other key area of consideration is the four sub-types. These subtypes—power assertive, power reassurance, anger retaliatory, and anger excitation—are described in more detail in Stephenson and Walter, and Keppel and Walter.[1,2] Experience in physical crime has demonstrated that all crimes fit into one or more of the sub-types. There usually is a primary sub-type and there may be secondary sub-types with lesser weightings in a complicated crime.

The crime scene reveals the sub-type(s) and there may be indications that the crime has started as one sub-type and ended as another, further differentiating the potential suspects. This "spiking over" from one sub-type to another is easily seen in the digital aspects of the hybrid crime scene due to the ability to analyze computer use patterns and documents such as emails, Internet pages, and social network accesses/postings.

Once the timelines of the crime are established, the important suspects may be characterized using the same sub-type analysis as applied to the crime/crime scene. This reduces the field of suspects to those who exhibit congruent characteristics to the crime. Those primary suspects are then analyzed based upon their pre- and post-crime activities, again searching for congruence with the physical event, and a smaller, more manageable sub-set of credible suspects is likely to emerge.

CPCA is applicable to hybrid investigations where the perpetrator is unknown but a field of suspects exists as well as investigations where the perpetrator is known and support for interview/interrogation and prosecution is needed. The presenters have applied CPCA in actual investigations and are currently analyzing empirical data for statistical correlation with theoretical constructs.

References:

1. Stephenson, Peter, Richard Walter, "Cyber Crime Assessment," hicss, pp.5404-5413, 2012 45th Hawaii International Conference on System Sciences, 2012
2. *Profiling Killers: A Revised Classification Model for Understanding Sexual Murder.* Keppel, Robert D., Richard Walter**.** 417, s.l. : International Journal of Offender Therapy and Comparitive Criminology, 1999, Vol. 43.

Cyber Crime, Crime Assessment, Digital Forensics

** Presenting Author*