

Estimation of terrorist network size from email contacts using capture-recapture methodology

Trent L. McDonald¹, James E. Driskell²

¹ Western EcoSystems Technology, Inc., Cheyenne, Wyoming, USA

² Florida Maxima Corporation, Winter Park, Florida, USA

International terrorist networks are characterized by dynamic, cell-based organizational networks. Understanding and predicting a network's capabilities, resources, and extent are critical to controlling and containing their activities. In the past, social network analysis has been used to identify network structure and dynamics. However, traditional social network analysis approaches typically assume near-complete and full information regarding participants in the network, whereas available information about covert, terrorist networks is often based upon missing and incomplete data. Ignoring the problem of incomplete network data can lead to erroneous and possibly disastrous consequences. In this paper we describe methods to estimate the size of an elusive or covert network based on capture-recapture methodology. From these estimates, the fidelity of social network data can be gauged, and a determination made as to whether, and how many, as-yet unidentified members of a terrorist network exist. We focus on estimation in situations where one or multiple members of the network have been pre-identified, and contact records of those individuals have been collected. We assume contact records involve email and cell phone records, but the methods are generally applicable to all types of contacts (e.g., known meetings). Our methods involve an adaptation of continuous-time capture-recapture models akin to the robust-design wherein individual contacts (emails) are viewed as secondary sampling occasions, known terrorists are the primary occasions, and additional contacts in the primary occasions are accumulated continuously through time. We apply the method to email traffic of a small business and cell phone records of a college fraternity's pledge class.