Criminal Investigations and Network Analysis
A DHS CENTER OF EXCELLENCE

GEORGE MASON UNIVERSITY

GeorgiaStateUniversity

The Next Battlefield: Illicit Markets Hosted on Encrypted Communication Platforms

LEAD PI: DAVID MAIMON

Criminal Investigative Processes

SUMMARY

As law enforcement agencies (LEAs) have gained traction in shutting down darknet markets and arresting operators, criminals are moving more of their operations to Encrypted Communications Platforms (ECP), which are not only easy for bad actors to create and use, but they are much more difficult for investigators to detect and shut down. LEAs require knowledge about the criminals who use ECPs, including their social networks and supply chains, and an evidence base in what works to thwart them. This project enhances law enforcement's ability to investigate and stop criminal activity by developing strategies for gathering intelligence from ECPs more effectively and efficiently.

PROBLEM STATEMENT

Encrypted Communication Platforms (ECPs) are used by criminals to significantly reduce investigators' ability to lawfully monitor communications relating to possible criminal activity. To enhance DHS's ability to investigate and stop criminal activity on ECPs, this project will generate knowledge about the criminals who use them, including the structure of their social networks and supply chains, and provide an evidence-based assessment of options to thwart them. The project will collect and analyze quantitative and qualitative data from ECPs on how illicit markets expand and persist over time, operate, and respond to interventions. This research will inform DHS's efforts to develop and implement evidence-based strategies for gathering intelligence from ECPs, analyze the intelligence in a cost-effective manner, and disrupt illicit online markets using ECPs.

APPROACH

Drawing on the research group's expertise and track-record of success in cybercrime detection and prevention, this project will complete six key research tasks:

1. Collect and assess data on ECP illicit markets, entities, and operations.
2. Assess ECP illicit markets' viability and trends (e.g., lifespan, growth, and decline).
3. Map the network of ECP illicit markets' entities.
4. Track entities' movements across ECP "channels" (akin to a chat room or instant message apps for groups).
5. Build artificial intelligence (AI) tools to summarize topics and correlate discussants.
6. Assess the effectiveness of disruption strategies on targeted markets and their participants, building on knowledge from prior DHS sponsored research.

ANTICIPATED IMPACT FOR DHS

This project will benefit investigators in three ways. First, the researchers will develop a large database of illicit markets using ECPs, including information on entities, products, and prices over time and across channels. This information will allow the identification and monitoring of trends and critical nodes. Second, the project will provide real-time information on the emergence and evolution of entities involved in the sale and purchase of illicit items and services or otherwise involved in crime, leading to the future potential of real-time alerts and identification of critical actors and threats. Finally, this project will provide one of the first evidence-based approaches to assess the effectiveness of network disruption strategies on illicit ECP markets. The team will release developed tools, source code, analysis, and aggregated data to stakeholders and the public as appropriate and allowed.