International Criminology Conference

Tim Pappa

Proposing a Conceptual Narrative Model Encouraging Whistleblowing Among Generational Cybercriminals Supporting Governmental Espionage

Cybercriminals supporting governmental intelligence and military espionage who are encouraged to become whistleblowers could singularly disrupt the global and geopolitical order. The scale of their access to or knowledge of sensitive information if shared publicly could abruptly reestablish geopolitical norms overnight and disrupt nation state disinformation efforts. The contemporary norms of cyberespionage suggest that espionage is generally not considered an act of war, therefore whistleblowers who appear to be acting independently could be considered an agnostic geopolitical event and role player in a world where leaking has precedent. This presentation suggests perhaps counterintuitively that encouraging these cybercriminals to become whistleblowers by demonstrating real and imagined peer whistleblowing of corruption and abuse could provide some balance, as many nations become more transparent even when forced because they lack information on what negative or questionable information will be revealed. There are changing generational norms suggesting that younger generations in different countries are more willing to vocalize allegations or evidence of fraud and corruption within their organizations, which is much more consistent with whistleblowing behaviors found in literature. The dynamic of a cybercriminal supporting governmental espionage may be different in terms of organizational affiliation, but there are still cultural and relationship considerations for cybercriminals weighing the impact of their cybercriminal support to governmental espionage in their own lives and others. This exploratory unorthodox position presentation integrates the research on the changing generational whistleblowing norms and models of shame and guilt influencing behavior in various cultures, proposing a behavioral paradigm for how cybercriminals could be motivated or encouraged to become whistleblowers, and how whistleblowing could continue to emerge as a naturalizing act that diffuses undemocratic and adversarial postures of international political and military decisionmakers. This presentation will demonstrate the application of this proposed narrative conceptual model to a theoretical scenario where there is corruption and abuse uncovered in governmental espionage.

Presentation outline:

Introduction

- Commentary and analysis on the impact of whistleblowing and leaks on geopolitical environments
- Examples from various countries and cultures, of non-cyber and cyber facilitated whistleblowing and leaking
- Recent literature on cyber and cyberespionage norms and the impact of cyber threat activity on global and geopolitical events and decision makers
- Considering cybercriminals and hacktivists who ‘leak’ stolen data and information and their motivations

Proposed integrated behavioral paradigm

- Exploring the historical and contemporary research into whistleblowing behaviors, including in Asian cultural contexts, specifically China
    - There are consistent whistleblowing behaviors in Asian and non-Asian contexts, contrasting some of the popular notions of who whistleblowers usually are
- Exploring the cultural models of shame and guilt in Asian contexts, and how shame and guilt influence behavior in those specific relational and public environments
    - Exploring contrasting and similar cultural models of shame and guilt in other global contexts

- Considering literature on theories on peoples' attitudes and decision making, such as Theory of Planned Behavior, but including how anticipated regret influences behavioral intentions.
    - Exploring a Chinese context of 'anticipated shame' as a mechanism of persuasion
    - Exploring a context of 'anticipated shame' or 'anticipated regret' in other contexts, such as military environments

Shaping a conceptual narrative model for encouraging cybercriminal whistleblowing

- Exploring the literature narrative persuasion as a conceptual framework
- Anecdotal application of this framework in strategic messaging to cybercriminal audiences, as an FBI profiler (former) specializing in online influence
- Visualizing the model when integrated with this behavioral paradigm related to whistleblowing behaviors and shame and guilt models
- Application of this conceptual narrative model to a theoretical scenario