

Thematic Workshop: Mock Botnet Investigation (World Federation of Scientists/ITU)

Tuesday, 17 May, 09:00–10:30, Room IX

A multidisciplinary group of international experts conducted a mock investigation of a botnet with the goal of bringing the audience closer to the difficulties in tracking and tracing cybercriminal activities, especially those that span multiple jurisdictions. The scenario was based around the theft of highly confidential medicinal formulas from an international pharmaceutical company. Three jurisdictions of the corporation were compromised, and the company had received an extortion email requesting USD 5 million for return of the formulas. The interplay with the general counsel of the company, the company's private forensic investigator, domestic law enforcement, foreign law enforcement, and the IMPACT global cybersecurity centre highlighted the complex jurisdictional issues, variances in cybercrime laws, and difficulties in investigating cybercrimes within a legal process designed for more traditional forms of crime. Mutual Legal Assistance Treaties and Letters Rogatory processes are time-consuming and hinder the ability to track and trace cybercrimes. The value of breach plans, inventories of data, and established relationships with law enforcement and providers was a central theme of the program. In addition, the panel demonstrated the critical role that IMPACT can play in facilitating 24/7 connections and sharing research and cyber investigation information.