POLICY INNOVATION CENTRE ROUNDTABLE AT STRATHMORE LAW SCHOOL JANUARY 16TH 2018.

Investigating and Prosecuting Cyber Crime: Identifying systemic impediments which obstruct police investigations, prosecutions, and digital forensics interrogations.

Introduction

With escalating reports of serious cyber-crimes in Kenya, one would expect to see a corresponding increase in conviction rates. However, this has not been the case with many investigations and prosecutions failing to take off. The key causes of this eventuality may be attributable-amongst others- to the challenges of cooperation between law enforcement agencies and information communication technology/service providers (ICT/S), trans-jurisdictional barriers, victimology and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime.

The ease with which cyber-crime crosses national borders, the seemingly irreconcilable differences between national legal frameworks, and the deceptions employed by cyber criminals impede attribution (customarily location based), and prevents law enforcement agencies (LEAs) from interrogating suspects and apprehending offenders.

Cyber-crime offending can be technically complex and legally intricate. Rapid advancements in the functionality of information communication technologies (ICTs) and innate disparities between systems of law globally are discrete challenges for investigating authorities, forensic interrogators, prosecuting agencies, and the adjudicative administrators of criminal justice. It is therefore critically important to explore the factors impeding investigation and prosecution of cyber-crime offending to raise awareness and expose these barriers to justice.

This roundtable seeks to examine criminal justice responses to cyber-crime under the common law model. The capacity of criminal justice actors to perform their core function will be analyzed and discussed.

Key Topics for the roundtable.

1. A practical definition of cyber-crime.
2. Investigative techniques and operational challenges.
3. Cooperation between information society service/technology providers and LEA's.
4. An evaluation of the evidentiary issues surrounding collection and presentation of electronically stored information (ESI).
5. Mutual legal assistance.
6. Recommendations for removing barriers to the effectiveness of cyber-crime inquiry.

Special focus: cybercrime and gender

1. Gender related cyber-crime offences.
2. Victimology and impediments to cyber-crime reporting