Social Cyber Forensics: Discovering Hidden Connections, Information Flows, And Information Actors In The Modern Information Environment

Tutorial Presenters:

1. Nitin Agarwal, Maulden-Entergy Endowed Chair Professor of Information Science, UALR, nxagarwal@ualr.edu
2. Samer Al-khateeb, Doctoral Candidate, Information Science, UALR, sxalkhateeb@ualr.edu
3. Muhammad Nihal Hussain, Doctoral Candidate, Information Science, UALR, mnhussain@ualr.edu

Abstract:

In today's information technology age, our thoughts, behaviors, and political discourse are highly influenced by what we see and read on our computer or smartphone screens. For instance, a fake or photoshopped image could be insidiously misleading. Misinformation is rampant in the modern information environment. Complemented with the availability of inexpensive and ubiquitous mass communication tools, such as social media, conducting deviant acts becomes both convenient and effective. For instance, deviant groups use social media to coordinate cyber campaigns in order to achieve strategic goals, influence mass thinking, and steer perspectives about an event.

In this tutorial, we present two case studies, i.e., influence operations of Daesh (ISIS/ISIL: Islamic State in Iraq and Syria/Levant) and Novorossiya. Each case study contains three events that were studied to gain situation awareness for the events. We introduce the methodology we followed to analyze each of the events and present the findings. We employ cyber forensics and computational social network analysis informed methodologies to identify and study influential information actors and competitors. Through cyber forensics analysis, we extract metadata associated with propaganda-riddled websites. The metadata assists in extracting the social network information (i.e., friends and followers) and communication network information (i.e., network depicting the flow of information) among the actors. Information from cyber forensics helps us conduct cross-media analysis, i.e., extracting Twitter profiles from blog profiles and vice versa. The information is then fed to Blogtrackers tool to identify popular trends; assess tones, sentiments and opinions; extract entities and analyze their networks. Through computational social network analysis, we identify influential actors and powerful groups coordinating the disinformation campaign.

Topics To Be Covered:

- We will introduce the concept of Social Cyber Forensics (SCF) and its effectiveness in collecting metadata.
- We will train the audience on a cyber forensic tool (i.e., Maltego) that can be used to study the cross-media affiliation and to uncover hidden relations between different groups.
- We will train the audience on social media monitoring tool, especially monitoring and tracking blogs (i.e., Blogtrackers) that can be used to further dig into the information obtained via cyber forensic analysis.
- We will provide a set of methodologies that can be followed to analyze a particular cyber information campaign.

- We will demonstrate the efficacy of the methodologies through case studies that examines the influence operations and disinformation or propaganda campaigns of ISIL and anti-NATO propagandist groups.

Special Constraints:

Systems requirements to Run Maltego CE and Blogtrackers are:

- Windows 7 or above, Mac OS X or above, or the latest version of Linux operating system
- Java 8.0 (or the latest version)
- At least 2GB of RAM, but the more the better.
- Any modern multi-core processor will be ok.
- 4GB of disk space is adequate.
- Mouse to make navigating the graphs much easier.
- Internet access is required to operate fully. Note that the outgoing connections will be on the following ports: 80, 443, 8081. Also, port 5222 is needed sometimes to join shared graphs on Paterva's public Comms server.