Analyzing Multimedia-based Disinformation Campaigns Conducted on Multiple Social Media Platforms

Tutorial Instructors:
1. Muhammad Nihal Hussain, Doctoral Candidate, Information Science, UALR, mnhussain@ualr.edu
2. Samer Al-khateeb, Assistant Professor of Computer Science, Department of Journalism, Media, and Computing, Creighton University. sameral-khateeb1@creighton.edu
3. Rick Galeano, Lieutenant Colonel, US Army, richard.a.galeano.mil@mail.mil
4. Katrin Galeano, Doctoral Student, Information Science, UALR, kkaniagalea@ualr.edu
5. Nitin Agarwal, Maulden-Entergy Endowed Chair Professor of Information Science, UALR, nxagarwal@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. Multiple social media platforms are used in an orchestrated manner to conduct disinformation campaigns. Various studies have been conducted to analyze such campaigns. However, most of the studies primarily focus on a single social media platform. These studies analyze how information flows within that platform but information flows across multiple platforms are largely ignored. Each social media platform is analyzed independently, even though content from one platform is shared or disseminated on others. These explicit cross-media linkages create a multi-layered content network that promises a holistic situation awareness of the disinformation campaign. A variety of social media platforms (e.g., blogs, Twitter, YouTube, Facebook) are strategically used to coordinate disinformation campaigns. Most studies have analyzed the role of Twitter in conducting disinformation campaigns. However, given the transition of information consumption behaviors from reading to viewing (blogging to Vlogging), it is imperative that video-based platforms are systematically studied. YouTube is one of the increasingly popular platforms exploited by adversarial information actors for pushing extreme contents, catering to a specific demographic (teens and youth, primarily) subjecting them to conspiracy theories, disinformation campaigns, and radicalizing content. Prolific linking of YouTube videos in tweets, blogs, Facebook, etc. has tremendously helped frame the discourse and is considered an extremely successful information operation tactic. This tutorial aims to peel the layers of the complex media integration strategy, demonstrate novel ways to assess the persuasive power of individual layers, and collectively assess their effectiveness in disinformation campaigns by leveraging conventional social network theories, social cyber forensic methodologies, and text mining.

Topics to Be Covered:

- Social Cyber Forensics (SCF) and its effectiveness in collecting metadata will be introduced. We will train the audience on a cyber forensic tool, i.e., Maltego that can be used to study the crossmedia affiliation and to uncover hidden relations between different groups.
- Blog monitoring tool viz Blogtrackers will be introduced. We will train the audience on monitoring and tracking blogs, identify posting trends, conduct opinion and sentiments analysis, identify influential bloggers and leading narratives, and analyze blog networks.

● Analysis of video-based social media platforms such as YouTube will be introduced via YouTube Tracker tool.

We will train the audience on monitoring and tracking content posted on YouTube, identify posting and content engagement trends (e.g., views, likes, dislikes, and comments), analyzing commenters' roles (prolific, cliques, brokers, etc.) and behaviors (bots, trolls, etc.), conduct opinion and sentiments analysis, extract cross-media affiliations, conduct related video analysis to detect possible algorithmic manipulations, and other such analyses.

● Case studies examining the disinformation campaigns during NATO exercises will be used to demonstrate the efficacy of the aforementioned methodologies.

● Interoperability among the tools will be demonstrated.

Special Constraints: Systems requirements to run the aforementioned tools 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