Social Media Networking and Tactical Intelligence Collection in the Middle East

Karen Howells, Near East University, Nicosia, Cyprus

https://orcid.org/0000-0002-8270-5279

ABSTRACT

Social media platforms are commonly used as a way to gather intelligence information by intelligence organizations in many countries. The data available from social media networks has been instrumental in aiding the organisation of rebellious activities in a number of Middle East countries. This article features an overview of the use of social media platforms in facilitating civil unrest, leading to an in-depth depiction of the use of such platforms both in Israel and the Palestinian Territories. After analyzing the types of data collected by intelligence agencies in the region, a model for filtering social network data through the use of socialbots is suggested. Using artificial intelligence, it is possible to design, create and build socialbots that can scrutinise enemy or terrorist organisations’ data output. Further programming would allow these socialbots to interact with a target and would be able to disseminate propaganda for the intelligence agencies.

KEYWORDS

Middle East, Social Media, SOCMINT, Tactical Intelligence

INTRODUCTION

Social Media Platforms are commonly used as a way to gather intelligence information by intelligence organizations in many countries, a process named SOCMINT, or Social Media Intelligence, a phrase coined by Omand et al. in 2012. SOCMINT describes the collection of openly available data that has been created by users of social media, in the context of bringing sensitive information to the attention of national intelligence services, as well as the sharing of information between governments and citizens (Omand et al., 2012). The data available from Social Media Networks, particularly Twitter and Facebook, has been instrumental in aiding the organisation of rebellious activities in a number of Middle East countries, especially in the Arab Spring revolutions in Egypt and Tunisia in 2011.

This paper features an overview of the use of Social Media Platforms in facilitating civil unrest in a number of Middle Eastern countries since 2010, leading to an in-depth depiction of the use of such platforms both in Israel and the Palestinian Territories. The amount of data freely available from such social networks grows on an hourly basis. Only a small proportion of this data is of significant interest to intelligence agencies, as part of their programs of surveillance. After analyzing the types of data collected by intelligence agencies in the region, a model for filtering social network data...
through the use of socialbots is suggested. Using artificial intelligence and other software, it is possible to design, create and build socialbots that can scrutinize enemy or terrorist organisations’ data output. This paper proposes that in combining socialbots with data mining, it is possible to build an effective software tool that would highlight a target population and could even communicate with and prompt the target to provide more information. Carefully produced socialbots would be capable of disseminating propaganda for intelligence agencies.

Currently it is estimated that there are 6000 tweets every second (Twitter Usage Statistics, 2018). Every 60 seconds there are 3.3 million posts on Facebook (Allen, 2017). Inside this massive amount of data are tweets and posts from concerned citizens, revolutionaries, and possible terrorists as they tweet and post their views and opinions. Any affixed photographs could contain the geo-location of their whereabouts. Photos with vehicles could reveal the registration plate of the vehicle, providing extra information for intelligence gathering. With these types of posts and tweets, it would be very easy for a terrorist or similar to find and locate a target. Civilians could also post photos of military operations, showing the insignia of the military unit, as well as geo-location. Social media information can be an effective tool in tactical intelligence collection for the military, and intelligence agencies, as well as for insurgents. From 2009, social media platforms were used by anti-government groups in the Middle East, to different levels of success (Shirazi, 2013).

As well as national security intelligence agencies using SOCMINT, it is used by non-governmental organisations. The United Nations also used SOCMINT to a large extent to plan a campaign to aid activists in Libya in 2011 (Sotlemyre & Sotlemyre, 2012).

Differing social media platforms have different types of data that may be of interest to SOCMINT gatherers. An individual’s Facebook profile can be a useful tool in intelligence surveillance. A user may be monitored through their posts, likes, shares, or through a new function called a “story”, where they may choose to publish a photograph or video that can be viewed for up to 24 hours. Connections between individuals on social networks such as Facebook can be analysed. Even where friendship is not obvious, it can be implicit through liked photos or comments. The friendships and likes awarded to posts in Facebook can be analysed as a network graph, and it would be possible to analyse the influence of certain individuals over time, as social network analysis can reveal hidden relationships in a Facebook network (Akhtar et al., 2013).

**SOCMINT IN THE MIDDLE EAST**

Cheong and Lee (2011) suggest that the use of Twitter by terrorists is minimal, but more recently insurgents and activists are increasingly moving to social media platforms to gather information, release propaganda and recruit like-minded people to their cause. By 2014 many insurgents in Iraq and Syria were using Twitter as a platform for disseminating propaganda, with foreign insurgents frequently retweeting already tweeted comments (Klausen, 2015). Insurgents in Iraq and Syria also used many different social media platforms and file sharing software, including Ask.fm, Facebook, Instagram, What’sApp, Pal-Talk, kik, Viper, JustPast.it., and Tumblr, and in addition to this Klausen (2015) discloses that encryption software is also used by insurgents.

Twitter was first engineered as an SMS platform, making use of the messaging sector of the GSM mobile telephones (Mahoney & Tang, 2016, 250). Twitter is low cost, easy to use, and tweets can now contain images as well as text, and links to other platforms. Tweets can easily be forwarded to all members of an address list. While most social media platforms need 3G or some Wi-Fi access, Twitter can work at the lower level of 2G GSM mobile networks (Klausen, 2015).

The managers of the insurgent Twitter accounts could be anywhere in the world, and they put on such an air of authenticity that Journalists often quote what they read on Twitter (Klausen, 2015). However, while these accounts seem spontaneous and authoritative, they are in fact the work of senior militants. New recruits give up their mobile phones when they arrive at the training camps, as do recruits in many modern regular armies, and so are unable to tweet.
Guide for Modelling a Network Flow-Based Detection System for Malware Categorization: A Review of Related Literature
www.igi-global.com/chapter/guide-for-modelling-a-network-flow-based-detection-system-for-malware-categorization/228470?camid=4v1a

IT Security for SCADA: A Position Paper
www.igi-global.com/article/it-security-for-scada/141224?camid=4v1a