ABSTRACT

The increased adoption of social media has presented security and law enforcement authorities with significant new challenges. For example, the Swedish Security Service (SÄPO) asserts that a large proportion of radicalization takes place in open fora online. Still, approaches to contain social media-driven challenges to security, particularly in democratic societies, remain little explored. Nonetheless, this type of knowledge may become relevant in European countries in the near future: Amongst other factors, the challenging economic situation has resulted in increased public discontent leading to emergence or manifestation of groups that seek to challenge the existing policies by almost any means. Use of social media multiplies the number of vectors that need law enforcement attention. First, a high level of social media adaption allows groups to reach and attract a wider audience. Unlike previously, many groups today consist of a large but very loosely connected network. This lack of cohesion can present a challenge for authorities, to identify emerging key actors and assess threat levels. Second, a high level of mobile web penetration has allowed groups to ad-hoc organize, amend plans and redirect physical activities. Third, the tool social media is as not exclusive to potential perpetrators of unlawful action, but is as well available to law enforcement authorities. Yet, efficient utilization of social media requires a deep understanding of its nature and a well-crafted, comprehensive approach. Acknowledging the broad functionality of social media, as well as its current status in the society, this article describes a model process for security authorities and law enforcement work with social media in general and security services work in particular. The process is cyclic and largely modular. It provides a set of goals and tasks for each stage of a potential event, rather than fixed activities. This allows authorities to adapt the process to individual legal frameworks and organization setups. The approach behind the process is holistic where social media is regarded as both source and destination of information. Ultimately, the process aims at efficiently and effectively mitigating the risk of virtual and physical violence.

Keywords: Law Enforcement, OSINT, Social Media, Swedish Security Service (SÄPO), Violence

DOI: 10.4018/ijcwt.2014040103
INTRODUCTION: SOCIAL MEDIA AND SECURITY

The rapid development of computer networks during the past decades has left its traces in many, if not all, areas of our lives. In a 2012 report compiled by the Boston Consulting Group analysts have estimated that by 2016 the number of Internet users will globally reach the 3 billion mark (Dean et al., 2012), a report authored by Scott Bicheno of Strategy Analytics appraised that the number of smartphones in use globally passed the 1 billion mark in the third quarter of 2012 (Reisinger, 2012). The ever-developing connectedness changed, and continues to change, the way we work, the way we entertain ourselves and the way we communicate.

The Internet “has become an ingrained feature of everyday life” (Dean et al., 2012) in many parts of the world. Sociologist Manuel Castells (2009) calls this the rise of mass self-communication. According to him, mass self-communication possesses certain socio-political power, which he exemplifies with so-called “grassroots”-movements that emerge in the society and grow with the help of shared information within the connectedness and have the potential to influence higher levels in the political system. Indeed, the global interconnectedness “is associated with greater citizen commitment to democratic governance,” according to Nisbeth et al. (2012). But with power to influence and change comes also the power to threaten and destroy, and thus, the potentially harmful aspects of the Internet, and the social media within, began to play a role in political practice, governance and in the related research, as an extension of the physical arena. This relatively new space is also a reflection of large parts of the global society, many of the actors seeking gain or influence in the physical world are today found online - from states to individuals, from organized terror organizations and hooligans and petty criminals.

Recognizing the importance of the new virtual domain, various authorities have shown an increased interest in utilizing cyber in general, and social media in particular, in their work. The virtual reality, however, have tasked organizations to amend their practices to fit its unique features and possibilities. Various methods have been developed and many authorities are nowadays are present in social media and seek to inform (Polisen 2011; Borchers 2011) or take advantage of social media’s two-way communication and seek out for public support in crime investigation (Vancouver Police Department 2011). Arguably, as comprehensive and interconnected the virtual world has become, as comprehensive the approach to work within should be in order to make efficient use of the opportunities as well as to address the pitfalls it offers.

This article seeks to present a process for security and law enforcement authorities to work with social media as a significant part of the virtual arena based on the various opportunities it offers. Because social media can be used for a wide range of purposes, the process was designed as general and flexible as possible in order to be implementable across various authorities with different responsibilities and limitations. Further, the process recognizes the need for the relevant authorities to cooperate and create shared situational awareness particularly during a significant event, in the sense of “shared awareness of a situation,” implies that authorities understand a given situation in the same way (Nofi 2000).

Despite its abstractability, process is largely based on various approaches to mitigation of large-scale public action, such as protests or mass violence. Unlike insight into issues closely aligned with national security, the work containing unrest is largely visible and tends to be thoroughly scrutinized in population, media, as well as academia. The recent years’ events, such as the riots in the UK in 2010 (Gross 2011), the events of the Arab Spring (Zuckerman 2011), as well as the Russian election-related protests in 2011/2012 (Jaitner 2013) have provided a rich empirical base of activities within social media. Arguably, the mechanisms derived from this empirical base are of use beyond addressing riots or mass violence. Consequently, the
Related Content

A Strategic Framework for a Secure Cyberspace in Developing Countries with Special Emphasis on the Risk of Cyber Warfare
www.igi-global.com/article/a-strategic-framework-for-a-secure-cyberspace-in-developing-countries-with-special-emphasis-on-the-risk-of-cyber-warfare/135270?camid=4v1a

www.igi-global.com/chapter/bio-cyber-machine-gun/7471?camid=4v1a

Infrastructures of Cyber Warfare
www.igi-global.com/chapter/infrastructures-cyber-warfare/7437?camid=4v1a
Cyber Can Kill and Destroy Too: Blurring Borders Between Conventional and Cyber Warfare

[www.igi-global.com/article/cyber-can-kill-and-destroy-too/124130?camid=4v1a](http://www.igi-global.com/article/cyber-can-kill-and-destroy-too/124130?camid=4v1a)