Chapter 28
Social Media Activism From an Information Warfare and Security Perspective

Brett van Niekerk
University of KwaZulu-Natal, South Africa

ABSTRACT

The use of social media in advocacy, and particularly transnational advocacy, raises concerns of privacy and security for those conducting the advocacy and their contacts on social media. This chapter presents high-level summaries of cases of social media in advocacy and activism from the perspectives of information warfare and information security. From an analysis of these, the impact and relationships of social media in transnational advocacy and information security is discussed. Whilst online advocacy can be considered to be a form of information warfare aligned to a Cyber Macht theory, it can be argued that social media advocacy negatively impacts information security as it encourages various actors to actively attempt to breach security.

INTRODUCTION

Social media's primary purpose is that of information sharing, be it amongst friends, family, or colleagues. However, the prevalence that social media has gained in contemporary society raises a number of concerns related to privacy and information security at personal, organizational and national levels. A number of cases exist which show that social media is actively being aligned to military operations as a 'force multiplier', indicating its use in information operations and information warfare. When considering advocacy and transnational advocacy, the use of social media immediately begins to raise the concern over information security for both the advocates, the targets, and others who get swept up in the online dialogue, and often the physical consequences that follow.

This chapter is an opinion piece based on previous research by the author and news reports of more recent cases; the fact that the incidents occurred is the relevant aspect to this chapter. The incidents are analysed based on the information security and information warfare models, from which key relationships

DOI: 10.4018/978-1-5225-7909-0.ch028

between social media advocacy and information security can be inferred. The next section provides an overview of information security and information warfare with particular reference to the models against which the incidents are analysed. A number of cases involving social media advocacy and information security are then outlined, followed by a discussion on the impact transnational social media advocacy has had on information security.

INFORMATION SECURITY AND INFORMATION WARFARE: AN OVERVIEW

Information security is the preservation of the confidentiality, integrity and availability of information and the relevant systems. Essentially this means that information can only be accessed by those who have authorization to do so, there needs to be accuracy and assurance only authorized persons can modify it, and it needs to be available when the authorized persons require it. Another important concept is that of non-repudiation, which is a form of attribution in that someone cannot deny their involvement or action, akin to a signature on a piece of paper.

Information operations and information warfare are military activities to provide information superiority over an adversary, including deception, psychological operations, intelligence and counter-intelligence. Of these activities, cyber-warfare has become predominant in the media due to the threat of online attacks. Cyber-security and information security are often used synonymously, although they are not identical. Information security is concerned with information in all its forms; a relevant concept of information warfare is that it operates in the physical, virtual and cognitive domains. Cyber-security, however, is concerned primarily with activities occurring on networks, and according to the ISO/IEC 27032 Cybersecurity standard, it is a subset of information security.

When discussing cyber-warfare and cyber-security, Duggan (2016) contrasts the US approach which is based on structure Jominian and Clausewitzian military theory versus the Chinese approach based on Sun Tzu's *Art of War*. Duggan (2016) attributes the apparent challenges experienced by the US due to the structured nature of their philosophy, and the apparent Chinese success due to the deceptive and unpredictable basis of their theory. The Chinese therefore have a stronger emphasis on social and psychological aspects of cyber-warfare, versus the US tactical approach (Duggan, 2016). The Chinese approach is therefore ideal for the inclusion of social media, which can better leverage disinformation, deception, and social constructs. In this instance, the integrity of human mind is influenced, which is an important concept in advocacy.

The concept of Cyber Macht or Cyber Power (Armistead & Starsman, 2014) is the use of modern communication channels (including online or cyber-space) to project power in the form of global influence, or mass perception management through "information shaping" (Armistead & Starsman, 2015:14). The premise is that due to the open access to modern online communications this power also resides with smaller groups who can effectively transmit their messages using this medium (Armistead & Starsman, 2014). This is almost a combination and Sun Tzu's psychological approach and Clausewitz's (1832) concept of "war is merely the continuation of policy by other means". This theory is particularly pertinent when considering transnational advocacy via social media.