Chapter 12
Information Warfare in the 2013–2014 Ukraine Crisis

Brett van Niekerk
Transnet SOC Ltd and University of KwaZulu-Natal, South Africa

ABSTRACT

In November 2013 a series of protests in the Ukraine resulted in a change of government, which was followed by a pro-Russian incursion of Crimea in 2014 and an attempted breakaway by Eastern Ukraine. During this crisis information warfare tactics were used extensively, from propaganda and misinformation to cyber-attacks. The chapter discusses these information warfare activities based on reports, social media activity, and secondary data. The time period of interest is up to mid-May 2014, however subsequent major events are considered. An ‘ideal’ information warfare campaign and possible future repercussions of the conflict are discussed. The information warfare campaigns are discussed in relation to cyber-strategies. The impact of the cyber-strategies of the two nations involved and lessons learned will be discussed.

INTRODUCTION

Information warfare, and in particular cyber-attacks, have been used in Eastern Europe during significant political unrest and conflict. Due to the prevalence of cyber-attacks related to political events in the region, it is unsurprising that there was a strong online component when protests erupted in Ukraine in November 2013, both in support and opposing the pro-Russian government at that time. The incursion by pro-Russian forces into Crimea in February 2014 and subsequent political activity in the region sparked a number of strong online reactions which can be considered as information warfare. For the purposes of this chapter information warfare is considered to comprise of various functional areas, including (Brazzoli, 2007):

- Network warfare, or more commonly known as cyber-warfare, where computer networks are the weapons an targets;

DOI: 10.4018/978-1-4666-8456-0.ch012
• Electronic warfare, which resides in the electro-magnetic spectrum and includes jamming and eavesdropping of signals;
• Psychological operations, which aims at altering the perceptions of the target audience to be favorable to one’s objectives.

In addition, the concept of social information warfare is applicable. This can best be illustrated by the Arab Spring events, where online activity played a large part in mobilizing and co-coordinating protestors. The most notable of these events resulted in a change of government in Tunisia and Egypt (van Niekerk & Maharaj, 2013).

The Myriam-Webster Dictionary (2014) provides a short definition for strategy as “a careful plan or method for achieving a particular goal usually over a long period of time” and a more detailed definition: “the science and art of employing the political, economic, psychological, and military forces of a nation or group of nations to afford the maximum support to adopted policies in peace or war”. A cyber-strategy would therefore use online activity to leverage the political, economic, psychological and military aspect to achieve the desired goal. From the definitions of information warfare and its functional areas, a cyber-strategy can be considered to be online activities that have an impact on a target’s psychological, information, or physical systems. In addition, physical or psychological activities that impact the cyber-based activities can be included in a cyber-strategy. Stonesoft Security (2014) indicates that a cyber-strategy is one which takes advantage of online opportunities whilst mitigating risks from the online environment.

The chapter analyses the information warfare activities surrounding the Ukraine crisis, based on social media activity, reports, and secondary data on DoS attacks. The following sections describe the methodology and theories used in this chapter and provide a background to the region and the crisis. The sections thereafter discuss the influence of social media during the protests, the propaganda and misinformation focusing on the online aspects, the cyber-attacks, and other relevant activities. These sections are followed by a discussion and the conclusion.

METHODOLOGY AND THEORIES

The chapter presents a qualitative analysis of news reports, social media activity, and imagery to determine the flow of events during the crisis, specific incidents and their impact, and the strength and accuracy of reporting. Secondary data is used for cyber-attack data to illustrate the magnitude of the attacks. Two theoretical models underpin the analysis: the IW lifecycle model (shown in Figure 1) and the network warfare attack process. The IW lifecycle model was proposed in van Niekerk and Maharaj (2011) and used to analyze the Arab Spring events in van Niekerk, Pillay and Maharaj (2011). It is a two-layered model, allowing for the overlap of high-level concepts with specific implementations and technologies to conduct the activities. Context is a key factor, and the lifecycle ultimately influences the context, allowing for the closure of the lifecycle or for continuing iterations (van Niekerk and Maharaj, 2011). This model informs the structure of the chapter: the background equates to the initial context of the model. The first iteration can be considered as the protests, which altered the context resulting in a strong pro-Russian resurgence, ultimately leading to the breakaway of Crimea and the attempted breakaway of the Eastern regions of Ukraine. Pro-Russian online rhetoric provided a continuous driver of the context to support their aims.