Chapter 72
Offensive Information Warfare Revisited:
Social Media Use in Man-Made Crises

Eli Rohn
Ben-Gurion University of the Negev, Israel

Connie M. White
University of Southern Mississippi, USA

Guy Leshem
Ashkelon Academic College, Israel

ABSTRACT

Socio-technical forecasts that materialized are of particular interest, as they are based on basic principles that must hold true for a long time, and thus worthy of special attention. The exploitation of the Internet as a vehicle for psychological and physical battle has been anticipated ever since the Internet became a world-wide phenomenon. Its potential for abuse by terrorist groups motivated Valeri & Knights to compile a list of key predictions, without the benefit of the hindsight afforded by the post-millennial terrorist attacks on the USA & Europe, and before social media was conceived. This paper evaluates some of their predictions in light of the massive social media and network attacks that occurred in Israel and Syria. Additionally, the paper examines how attacked governments and nations respond. The authors find that some of the key predictions advanced by Valeri and Knights have proven accurate. Offensive information warfare attacks have and will continue to influence policies, budgets and civic voluntary participation to counter such attacks.

DOI: 10.4018/978-1-5225-7113-1.ch072

A lie gets halfway around the world before the truth has a chance to get its pants on. -Winston Churchill

INTRODUCTION

Socio-technical forecasts that materialized are of particular interest, as they are based on basic principles that must hold true for a long time. Such principles are usually rare and therefore are worthy of special attention, study and incorporation in the field's main body of knowledge. The use of the Internet and new media by militants and terrorists has been an active field of research (Arquilla & Borer, 2007; Denning 2007; Elovici, Kandel, Last, Shapira, & Zaafrany, 2004; Kandel & Last, 2005; Gabriel Weimann, 2014; Gabriel Weimann, 2015).

Only four years after the Internet became a recognized and useful tool on a global scale, Valeri and Knights (2000) made specific predictions about the types of militants that would use the Internet to advance their own causes and outlined how they would realize that goal, labeling these activities Offensive Information Warfare (OIW). Although the authors are aware of more recent work that has contributed related terminologies to the field (Stevens, 2012; Taddeo, 2012), the authors find the term OIW to be the most appropriate for this article.

According to Valeri and Knights (2000), OIW is defined as:

The set of activities carried out by individuals and/or groups with specific political and strategic objectives, aimed at the integrity, availability and confidentiality of the data collected, stored and transferred inside information systems connected to the Internet. They also provide specific criteria to further describe the conditions that will most likely foster the use of OIW:

1. Lack of an established and/or successful operational style,
2. Ability to foster an offensive OIW capability and/or
3. An enemy that is highly dependent on information systems

The ongoing turmoil in the Middle East has become not only a physical battlefield, but a proving ground for new-media exploitation and experimentation. Militant groups the world over explore how to best exploit online social media for support and for propaganda purposes.

Our paper evaluates some of the predictions made by Valeri and Knights using the 2012 violent conflicts in Syria and in Israel. That is because the Syrian and Israeli conflicts occurred within the same timeframe and in the same geographical region, but in two countries at vastly different stages of development. The choice of these events as our study focus facilitated using an experimental design that it is highly similar to those prevalent in social science research, namely, the 2×2 design, in which most variables are held constant, thereby allowing cause and effect (or lack thereof) to be better identified and explained.

Specifically, the authors examine the confrontation that erupted between Israel and Hamas in the Gaza Strip (November 2012) and the first eighteen months of the uprising and civil war in Syria (March 2011 – November 2012). With those events as the sources of our data, the authors focused on two issues that illustrate at once both the strengths and weaknesses inherent to the Internet as predicted by Valeri