Chapter 9

Xue Lin
University of Ottawa, Canada

Rocci Luppicini
University of Ottawa, Canada

ABSTRACT

Technoethical inquiry deals with a variety of social, legal, cultural, economic, political, and ethical implications of new technological applications which can threaten important aspects of contemporary life and society. GhostNet is a large-scale cyber espionage network which has infiltrated important political, economic, and media institutions including embassies, foreign ministries and other government offices in 103 countries and infected at least 1,295 computers. The following case study explores the influences of GhostNet on affected organizations by critically reviewing GhostNet documentation and relevant literature on cyber espionage. The research delves into the socio-technical aspects of cyber espionage through a case study of GhostNet. Drawing on Actor Network Theory (ANT), the research examined key socio-technical relations of Ghostnet and their influence on affected organizations. Implications of these findings for the phenomenon of GhostNet are discussed in the hope of raising awareness about the importance of understanding the dynamics of socio-technical relations of cyber-espionage within organizations.

INTRODUCTION

What these guys [corporate officials] don’t realize, because nobody tells them, is that a major foreign intelligence agency has taken control of major portions of their network. You can’t get rid of this attacker very easily. It doesn’t work like a normal virus. We’ve never seen anything this clever, this tenacious (Mills, 2010).

GhostNet was a cyber espionage network in 2008 that attracted much attention and raised serious public concern. The purpose of studying GhostNet here is to explore technoethical and communicative aspects of cyber espionage on affected organizations, which significantly influences cyber peace and corporate develop-
Socio-Technical Influences of Cyber Espionage

To investigate the socio-technical influences of cyber espionage, despite increased media attention on hackers and cyber espionage, little empirical research has been conducted on GhostNet. For example, Tracking GhostNet: Investigating a Cyber Espionage Network by Information Warfare Monitor (2009) examines the GhostNet phenomenon, focusing on the social and technological aspects and how GhostNet was tracked. To address this, this study adopts Actor Network Theory (ANT) to examine technical and communicative actors in a socio-technical process.

This analysis of socio-technical aspects of cyber espionage is guided by Actor Network Theory (ANT). ANT emerged in the mid-1980s with work primarily from Bruno Latour and Michel Callon, and significant later contributions from John Law (1999). ANT is a conceptual framework for exploring collective socio-technical processes, whose advocates have paid particular attention to scientific and technological activities. ANT suggests that the work of science is not fundamentally different from other social activities, instead asserting that it is a process of heterogeneous engineering in which the social, technical, conceptual and textual are juxtaposed and translated (Latour, 1991; Law, 1999).

As applied to this study, ANT suggests that several aspects should be studied: the actors of cyber espionage (behaviours), hackers (people) and technology (objects), as well as the network associated with these actors. Based on ANT, this research focused on socio-technical aspects revolving around how the GhostNet network was formed and how it fell apart. This research study utilizes a case study approach guided by the work of Yin (2003) and Creswell (2007) to carry out a comprehensive document analysis of relevant industry reports, research literature and other documentation pertaining to the case.

BACKGROUND
Cyber Espionage

Unlike previous, physical frontiers, cyberspace is a human construct. Cyber behaviours, such as cyber espionage, cyber surveillance, cyber terrorism, influence cyberspace significantly in different ways. “Cyber espionage is a technology by which system access is illegally obtained, data or computer equipment is stolen or destroyed, or software is illegally copied” (Stair, 1996, p. 529). Trojan horse programmes and other associated malware are often cited as tools for conducting sophisticated computer-based espionage.

Cyber space is a battlefield for information warfare with not only legal but also ethical implications. According to Mason (1986), the ethical issues of cyber space usually involve four areas of concerns: privacy, accuracy, property and access (PAPA):

Privacy—the ability of people to keep personal information about themselves private and confidential; how the widespread holding of personal information about people impacts on interpersonal relations of trust, autonomy, and dignity;

Accuracy—the quality and accuracy of data/information held in databases, and on which organisations act, assuming the data/information to be correct;

Property—information ownership and control—who owns personal information about an individual, and who has the right to use it, or control its use; and

Accessibility—access of members of society to the social store of information (Mason, 1986).

As an issue relating to ethical concerns and cyber crime, GhostNet entails two of the ethical charges, privacy and access.

Contemporary research in Technoethics extends to research on cyber ethics and topics such as online privacy, copyright, security, and surveillance. Cyberterrorism, and cyber espionage
Related Content

Use of the Secondary Task Technique for Tracking User Attention
www.igi-global.com/chapter/use-secondary-task-technique-tracking/13192?camid=4v1a

The Empathy Paradox: Increasing Disconnection in the Age of Increasing Connection
Sara Konrath (2013). Handbook of Research on Technoself: Identity in a Technological Society (pp. 204-228).
www.igi-global.com/chapter/empathy-paradox-increasing-disconnection-age/70356?camid=4v1a

B is for Bias: From Rational Maximizer to Homo Heuristicus
www.igi-global.com/article/b-is-for-bias/113838?camid=4v1a

E-Government for Social Inclusion?
www.igi-global.com/chapter/government-social-inclusion/64944?camid=4v1a