Chapter 16
The United Kingdom's Centre for the Protection of National Infrastructure:
An Evaluation of the UK Government's Response Mechanism to Cyber Attacks on Critical Infrastructures

Stuart Weinstein
University of Hertfordshire, UK

Charles Wild
University of Hertfordshire, UK

ABSTRACT

This chapter examines the effectiveness of the newly-formed CPNI in leading the United Kingdom's response to cyber attacks on critical infrastructures.

1. INTRODUCTION

On 25 June 2009, the UK Prime Minister[1] presented Parliament with a command paper entitled *Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space* (Cm. 7642). Recognising the challenges of cyber security and the need to address them, *Cyber Security Strategy* stresses the need for a coherent approach to cyber security. At the heart of the strategy is the role of the Centre for the Protection of National Infrastructure ("CPNI")[2] which was formed in order to deliver advice aimed at reducing the vulnerability of organizations in the national infrastructure to terrorism and other threats such as espionage, including those from cyber space (Cm 7642).

DOI: 10.4018/978-1-61520-831-9.ch016

The CPNI was formed from the merger of the National Infrastructure Security Coordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC) (CPNI Website 2009). Although CPNI was only formed on 1 February 2007, this work was carried on before by the NISCC and NSAC (CPNI Website 2009). The NISCC provided advice and information on computer network defense and other information assurance issues, whilst the NSAC provided advice on physical security and personnel security issues. The CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organizations that make up the national infrastructure (CPNI Website 2009). It is the mission of the CPNI to deliver advice to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats (CPNI Website 2009). Significantly, the CPNI is an interdepartmental organization with resources from a number of government departments and agencies including MI5, CESG (Communications Electronics Security Group) - the UK's National Technical Authority for Information Assurance and other Government departments responsible for national infrastructure sectors (CPNI Website 2009).

2. BACKGROUND

The CPNI is accountable to the Director General of the Security Service (MI5)[3] and operates under the *Security Service Act 1989,* providing expert advice to the critical national infrastructure on physical, personnel and information security, to protect against terrorism and other threats. Its key partners include businesses and organizations that own or operate critical infrastructure, government departments, security specialists and the police (CPNI Website 2009). In accordance with the Prime Minister's February 2005 statement[4], the Security Service has assumed the lead responsibility for all national security intelligence work in Northern Ireland from the Police Service of Northern Ireland (CPNI Website 2009). This transfer of responsibility brings Northern Ireland's arrangements for national security work into line with those for the rest of the UK (CPNI Website 2009). Under the new arrangements, CPNI will assume the lead for providing protective security advice to the national infrastructure within Northern Ireland, particularly relating to the delivery of advice to CNI operators covering physical, personnel and information security (CPNI Website 2009).

A fair amount of the focus of the CPNI is to warn critical businesses in the UK which operate computer systems, such as power companies and large financial institutions that these systems are being repeatedly probed to steal information or to uncover weaknesses that could take them down. For instance, Mark Oram, Head of the CPNI's Threat and Information-Security Knowledge Department, speaking at the RSA Conference Europe 2008 in London said: "We see frequent attacks on organizations for the purpose of theft of property. There are known threat sponsors with known requirements looking to gather information from industry" (Heath 2009). He went on to state that "The use of cyber-techniques is relatively easy, cheap and low risk in terms of being caught. Most of the time, we know the likely culprit but proving it is very difficult." He added however that the UK Government feels the risk of a cyber-terrorist attack is low due to a "lack of capability and difficulties with understanding the vulnerabilities in the infrastructure" (Heath 2009). Oram stated that the CPNI would continue to work closely with key industries, to help them understand the vulnerabilities and threats they face.

In contrast to Mr Oram's viewpoint, that the risk of a cyber-terrorist attack is low, Lord West of Spithead, the Security Minister, believes that a mixture of state-sponsored individuals and those operating at a terrorist level frequently try to break into the key UK networks. Intelligence organiza-