TYNE AND WEAR FIRE AND RESCUE AUTHORITY
EMERGENCY PLANNING UNIT
Committee Report

Meeting : CIVIL CONTINGENCIES COMMITTEE: 7 JULY 2008

Subject : WEBSITE MONITORING:TERRORISM

Report of the Chief Emergency Planning Officer

1. Introduction

1.1 Governments are increasingly aware that terrorists have fully exploited the modernisation of communications to their advantage, particularly the internet. It is known that prospective militants can make use of the internet to establish various forms of online, private, person-to-person or group communication - including chat-rooms, blogs, websites, and forums as an alternative (or preliminary) to travelling to Pakistan or other theatres of *jihad* to gain fighting experience.

1.2 Evidence strongly suggests that terrorists used the Internet to plan their operations for 9/11. Computers seized in Afghanistan reportedly revealed that al Qaeda was collecting intelligence on targets, and sending encrypted messages via the Internet. With regard to gathering information through the Internet, on 15 January 2003, US Defense Secretary Donald Rumsfeld observed that an al Qaeda training manual recovered in Afghanistan said, *"Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy".*

2 EPU Website Monitoring

2.1 The Emergency Planning Unit (EPU) website has proved to be an extremely popular website since its introduction in 2005, with over 20,000 unique visitors to the site who have downloaded over 56,000 pages. Other emergency planning units have sought permission to emulate the style, content and layout of the website.

2.2 The content of the website is reviewed and a management process in place to ensure that sensitive material is not published. A secure area for partners in the local authorities who have been issued with a username and password is used for more sensitive information.

2.3 It is important to stress that no sensitive information is published on the EPU website, and that all published data complies with legislative requirements. As a matter of routine, the EPU website is regularly monitored to detect any suspicious activity.

2.4 Activity such as lengthy visits to the website, regular viewing of the same documents or pages and regular visitors, particularly international visitors are all monitored and recorded. Using an online tool, the EPU tracks visitors and identifies their IP (Internet Protocol) addresses, which is the unique 'signature' left by the website user and gives their location and viewing patterns.

2.5 Nevertheless, recognising that the nature of the EPU's work is likely to attract interest from those persons who may wish to seek out information to be used for malicious purposes and to cause harm to others, a meeting was arranged with the Northumbria Police Counter Terrorism Security Adviser (CTSA) to review arrangements and ensure they were adequate.

3.0 Suspicious Activity

3.1 The Police CTSA confirmed that they were highly satisfied with existing levels of monitoring that are currently in place within the EPU.

3.2 Any information which could potentially be regarded as 'suspicious' is routinely reported by the EPU to the Northumbria Police Counter Terrorist Security Adviser (CTSA). To date the EPU site has had 'hits' which might be considered to be unusual, from the following locations:

> Iran, Iraq, Poland, Israel (West Bank), the Gaza Strip, Saudi Arabia, the Lebanon, and Singapore; with one 'hit' from mid-ocean. In addition, there have been extremely lengthy visits from two London IP addresses - which may simply be the consequence of a student or resilience officer forgetting to close a browser window. However this is still picked up during our monitoring and routinely reported.

3.3 Northumbria Police CTSA's keep track of and record those IP addresses which arouse suspicion and these are cross referenced with addresses that have been recorded for other related policing purposes. Should the CTSA consider that the information could possibly be terrorist related or be part of terrorist-related hostile reconnaissance activity, the information is forwarded to:

- the Counter Terrorism Command in Scotland Yard, where it is entered onto a computer database which identifies patterns of potential national and international terrorist activity; and
- the National Counter Terrorist Security Office (NaCTSO) Centre located within the Centre for the Protection of National Infrastructure (CPNI), located within the security services (www.cpni.gov.uk)

for analysis and action if required.

4 Conclusion

4.1 It is pleasing to note that the stringent management and monitoring procedures in place for the EPU website meets with the approval of the security services. The EPU will continue to monitor website activity in order to

maintain a pro-active approach to risk management and to assist the security services where possible.

5 Recommendation

5.1 Members are asked to note the robust arrangements in place and to note this report.

BACKGROUND PAPERS

www.twepu.gov.uk

www.cpni.gov.uk

www.nactso.gov.uk