A Multidisciplinary Conference on Cyberterrorism
Executive Summary – July 2013

The Cyberterrorism Project hosted a multidisciplinary conference on cyberterrorism at Jury's Inn Hotel, Birmingham, UK on 11-12 April 2013. Forty-eight delegates attended the conference, including researchers from a number of UK universities as well as institutions in the Republic of Ireland, Israel, Italy, the Netherlands, Romania, Sweden, Greece, Australia and the United States. Other attendees included representatives from Her Majesty's Inspectorate of Constabularies and the Welsh Government.

Summary of Findings

- Cyberspace opens considerable potential opportunities for terrorist activities, including communication, fund-raising and attacks.
- There are multiple constraints on terrorist engagements with cyberspace. First, the feasibility of the terrorist activities listed above varies considerably with some requiring very little technical knowledge and others necessitating a high level of expertise. In addition to this are further constraints such as financing and the comparative desirability of more traditional attacks for reasons of visibility or knowhow.
- A range of legal and political instruments are available within national and international bodies with which to confront the challenge of cyberterrorism. However, these instruments are limited by different factors including: different strategic cultures and capabilities across countries; the language and construction of existing legal instruments such as the 'use of force' requirement in international law; and, sensitivities towards sharing information and data.
- Distinguishing between different types of cyber-threat is challenging, in part, because motives and behaviour in this realm are difficult to identify and monitor.
- The value of existing models and methods of deterrence to confront challenges such as cyberterrorism is unproven, at best.
- Efforts to address threats such as cyberterrorism raise considerable ethical as well as political, legal and technical challenges.
- Cyberterrorism has a discursive existence as well as a 'material' one. How this phenomenon is framed or constructed in media and political language matters greatly.
- The disciplinary backgrounds and commitments of academics are not incidental within debate on the definition of cyberterrorism. In part, this is because of different views of the purposes of definition itself, which include: to ensure effective communication between researchers and/or policymakers; to facilitate cooperation across jurisdictional boundaries; to distinguish terrorism from crime and war; or, to impose limits on investigative and prosecutorial powers.

A full report detailing each paper, as well as further information on the conference and the project in general is available at:

http://www.cyberterrorism-project.org/

or email: ctproject@swansea.ac.uk

Follow the project at:

/CyberterrorismProject

@CTP_Swansea

This event was supported by: