# Terrorists' Use of the Internet – Executive Summary

The Cyberterrorism Project hosted a multidisciplinary symposium on terrorists' use of the Internet, at Swansea University, UK on 5-6 June 2014. Forty-three delegates attended the symposium, including researchers from a number of UK universities, as well as institutions in the Republic of Ireland, France, the Netherlands, Norway, Turkey, Canada and Australia. Other attendees included representatives from the Home Office, South Wales Police and the Scottish Organised Crime and Counterterrorism Police Unit.

## Summary of Findings

A wide range of topics were addressed, including the possibility of cyberattack, a variety of preparatory and support activities and questions of response. Across these diverse topics a number of themes were evident:

- **Definition:** There is a wide variety of understandings of key terms, including cyberterrorism. These diverse understandings not only have the potential to obscure discussion, but also have important practical ramifications (for example, in developing models of risk management). Deconstructing different understandings of cyberterrorism has the potential to open up a range of other important research questions and create space for dissident voices.
- **Transnational:** Many online terrorist activities, including publicity, propaganda, radicalisation and finance, now transcend national boundaries. As a result, international law has a significant role to play, and international cooperation is essential. At the same time, it is important to recognise that many terrorist groups have a specific geographical focus, as the tweets during the Westgate attack illustrated.
- **Decentralisation:** Terrorist activity is also increasingly decentralised. Examples include the outsourcing of propaganda production, bottom-up radicalisation and the growing number of self-funded terrorist cells.
- **Vulnerability:** Cyberspace itself is often presented as inherently vulnerable. Nation states, and in particular their critical infrastructures, are frequently portrayed as susceptible to attack. Citizens are often presented as being vulnerable too, in some cases to radicalisation and in others to cyberattack and cybercrime.
- **Credibility:** The credibility of terroristic narratives and counter narratives is important. So too is the credibility of governments' counterterrorism laws and policies, and the discourse surrounding these. This is particularly apparent in the case of cyber surveillance.
- **Power:** Terrorist groups employ both hard and soft power in pursuit of their objectives. Whilst counterterrorism frequently employs hard forms of response, there are concerns about the extent to which soft countermeasures are used and their effectiveness when they are employed.
- **Evidence:** Areas where understanding is currently lacking and further research is required include: terrorists' cyber capabilities and the materials they place online; the consumers of extremist online content; the relationship between the Internet and the offline world; the effectiveness of counterterrorism laws and policies, including accountability mechanisms and how to assess effectiveness; how counterterrorism policies are produced; and, how cooperation can be engendered between the private and public sectors and within the international community.

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:

Swansea University
Prifysgol Abertawe

Curtin University

Office of Naval Research Global Science & Technology