Cyber terrorism and war, the looming threat to the industrialised state

blogs.lse.ac.uk/waronterror/2011/06/16/cyber-terrorism-and-war-the-looming-threat-to-the-industrialised-state/

Posted by AD Brown

Earlier this month the EastWest Institute held its second worldwide summit on cyber security. Hundreds of government and industry leaders, from over 43 countries, attended to discuss the looming threat of increasing war and criminality within the cyber domain.

Major concerns focused around the impact a major cyber attack would have on the critical infrastructure that now supports daily life in industrialised countries. According to recent estimates, 1.8 billion people are now online, within 246 countries. Trillions of dollars are exchanged and vial public services, from networked hospitals to water and electrical services, are now highly dependant on networks and their computer counterparts. Prime example of this dependency was the cyber attack on Estonia in 2007. Within a matter of hours Estonia suffered a major and sustained cyber attack that lasted for over three weeks and brought its government to a halt. It was not until, with the help of NATO cyber terrorism experts, that Estonians were able to eventually regain their state services and secure their cyber infrastructure. The Estonia case, as a state highly dependent on providing government services via the internet, was a wake-up call to governments around the world to better secure their own infrastructures from such an assault.

The asymmetric nature of the cyber attack, makes cyber terrorism potentially very effective. Carrying out cyber attacks are comparably low cost to that of other forms of mass disruption and as the Stuxnet worm made evident, have potential to engage even nuclear assets. However, Stuxnet was purportedly a state creation, aimed at another state, so could this be argued to be an act of terrorism or war? Definitional agreement in the cyber domain is proving difficult to achive.

Profiling the cyber terrorist

Ascertaining who is a ‘cyber terrorist’ or what is ‘cyber terrorism’, is certainly still a problematic and unresolved dimension in the discourse of this new emerging threat. In a recent report on critical terminology foundations of cyberspace, cyber terrorism is defined as “…’the use of cyberspace’ for terrorist purposes as defined by national or international law”.

But defining ‘terrorism’ itself has proved a daunting task with hundreds of potential definitions. To use one established by US National Counterterrorism Center, terrorism is defined as

> *…premeditated; perpetrated by a subnational or clandestine agent; politically motivated, potentially including religious, philosophical, or culturally symbolic motivations; violent; and perpetrated against a noncombatant target.*

If we take word ‘cyber’, as used in the American context, that being ‘electronic infrastructure’ and combine it with the above definition of ‘terrorism’, we soon find almost any act committed via the intranet or cyber domain could be construed to be an act of terrorism.

‘Hacktivists’, for example, fall into this definitional grey zone. Hacktivists are often seen as ‘online’ protesters who carry out virtual acts of protest. Perhaps most famous, is the group known as Anonymous, who have, in response to the arrest of Julian Assange, attacked Mastercard and Amazon websites temporarily shutting them down. However,

as some commentators have pointed out, there is an element of civil disobedience to such actions and perhaps it is misleading to label these actions as being acts of ‘terrorism’ or ‘criminality’. For example, Mathias Klang has argued that Denial of Service attacks (a particular type of attack used by many hacktivists, including Anonymous, to temporally shut down websites) are a form of civil disobedience. Klang has termed these ‘protests’ as ‘virtual sit-ins’.

While hacktivists provide an academic challenge to definitional terms of cyber terrorism, there is no doubt that groups such as al Qaeda (AQ) within the ‘real world’ are terrorist organisations, at least in so far as they are the primary focus of the ‘War on Terror’. Interestingly, however, ‘traditional’ terrorist groups have not moved so rapidly into the cyber realm. Thus far, we have not seen large scale cyber terrorism methods used by AQ or other religiously motivated terrorist organisations on government targets. While AQ have certainly mastered the use of the internet to recruit young jihadists and promote their beliefs, they have seemingly stuck to more traditional ways and means of carrying out acts of terror (suicide bombs, IEDs). It is unlikely this trend will continue and one would predict it is only a matter of time before these groups adopt the use of cyber attacks as a means of terrorism.

In the closing remarks of the EWI’s cyber security summit, President John Mroz stressed that cyber challenges are ‘by definition’ global. This is an important point to take away from this emerging threat to the industrialised and increasingly dependant cyber state; that fighting cyber terrorism is and will involve all countries and the greater global civil society. It is truly a major twenty-first century threat to the international order and will require an equally international response.