A new phenomena of security challenges: Cyberterrorism and beyond

Interviews

November 11, 2013



Like 2,299 people like this.

JTW Interview, Assoc. Prof. Stuart Macdonald

JTW team has made an extensive interview with Assoc. Prof. Stuart MacDonald, Deputy Director of the Centre for Criminal Justice & Criminology at Swansea University . Mr. Macdonald is also the co-director of Cyberterrorism Project. For more information about the project: http://www.cyberterrorism-project.org/

Mr MacDonald, could you please explain briefly your Cyberterrorism Project?

The cyber terrorism project was established in 2011 by academics working across different disciplines from the social sciences, and the physical sciences, and we're keen to adopt a multidisciplinary approach to understanding cyber terrorism and the threat that it poses. To date, we have conducted a number of activities, we hosted an international conference earlier this year, and we have conducted a survey of the global research community, exploring understandings of cyber terrorism and evaluating responses.

We also have two edited collections that will be published in 2014. These include a number of papers that were presented at our conference earlier this year.

What were some of the findings in this project?

Our survey explored different issues.Firstly, in terms of understandings of cyber terrorism, it found that there are some dominant understandings but not unanimity. The majority of the respondents to our survey regarded definitions of terrorism, and of cyber terrorism, as being important. And also said that the definitions or issues around these terms have not been resolved satisfactorily yet.

Other dominant views were that motive, digital means or target, and fear in a wider audience are important features of cyber terrorism. Interestingly though, less than half of our respondents thought that phsyical violence against people or property is an important feature of cyber terrorism. This stands in marked contrast to studies of the concept of terrorism itself. And leads us to question whether adding the 'cyber' prefix to the parent concept of terrorism may lead us to question, perhaps even reconsider how we perceive terrorism in general.

Do you think that cyber terrorism will be a new phenomenon of security studies in the future?

This is a question that has really divided opinion. There are some that have given quite strong warnings of the threat that cyber terrorism poses.

At the other end of the spectrum there are those who are far more skeptical.Some argue that the threat is no more than hypothetical – claiming there is no empirical basis for the threat.

Some of the arguments given for the view that cyber terrorism is not a significant threatinclude cost(some studies have found that a cyber attack would be more expensive than a traditional physical attack). But also that a traditional physical attack is more attractive to terrorists, because of the kind of photographs and video images that it produces, as a publicity factor.

Others have argued that cyber attacks could be presented by authorities as merely an accident, or, maybe dismissed as anonymous attackers. This would then starve terrorist groups of the publicity that they crave and so cyber attacks would be unattractive to them for this reason, too.

Are there any new initiatives at UK and EU level in case of legal documents – producing legal documents or legal texts?

The UK actually introduced cyber terrorism to it's definition of terrorism in the year 2000, before the attacks of 9/11. That part of the UK's definition has been quite strongly criticised by UK commentators. It refers to serious disruptions or interference with electronic systems which, commentators have argued, sets the bar too low for many attacks could cause serious disruption but still fall some way short of what would

popularly be regarded as terrorism. More recently, the UK government has invested 650 million pounds in setting up a cyber security strategy. That was 2 or 3 years ago and there are now 8 centers of excellence for security research in the UK. So it is being quite an important part of public policy. The national security strategy for the UK identifies four threats in the top-tier of threat levels, and two of those four are 'cyber crime' and 'international terrorism'. So cyber terrorism is the convergence of two of what the UK regards as four of the most important threats to national security.

Which terrorist organization is using cyber terrorism most efficiently?

That is something that would really split opinion. There are many that would say that terrorist organizations have not used cyber attacks and they doubt whether they are actually exploring the possibility of cyber attacks at the moment. The kind of instances that have occured today, like the 'stuxnet incident' – these commentators would say that is not terrorism, because it appears it was perpetrated by states. But that then leads onto a further question, which is something we examined in our survey: the majority of respondents said that cyber terrorism could be carried out by states. So the traditional view that terrorist acts are acts committed by non-state groups also seems to be challenged by the phenomenon of cyber terrorism. It seems that we are more willing to regard cyber attacks by state actors as cyber terrorism than traditional physical attacks. That then raises the question of whether states can commit acts of terrorism.

Does a distinction have to be made between 'pure' cyber terrorism and the terrorist use of cyberspace?

In my view cyber terrorism should be conceived narrowly, because the criminal law penalizes many acts which are preparatory to acts of terrorism. If you regard acts of preparation as a substantive terrorist act, then acts which are preparatory to those acts would then be penalized by the criminal law as well. The criminal law would then apply to a very wide range of conduct, conduct that is very far removed from the actual attack itself.

By Reyhan Güner & Oğuz Kaan Pehlivan



0 Comments Sort by Top

Add a comment...

Facebook Comments Plugin