A Multidisciplinary Conference on Cyberterrorism

Final Report

July 2013

the cyberterrorism project

About the Project

The Cyberterrorism Project was established at Swansea University, UK in 2011 by academics working in the School of Law, College of Engineering, and Department of Political and Cultural Studies. The project has four primary objectives:

(1) To further understanding amongst the scientific community by engaging in original research on the concept, threat and possible responses to cyberterrorism.
(2) To facilitate global networking activities around this research theme.
(3) To engage with policymakers, opinion formers, citizens and other stakeholders at all stages of the research process, from data collection to dissemination.
(4) To do the above within a multidisciplinary and pluralist context that draws on expertise from the physical and social sciences.

The project's directors are Professor Thomas Chen, Dr Lee Jarvis, and Dr Stuart Macdonald. Its other team members are David Mair, Lella Nouri, Andrew Whiting, Joanna Halbert, Wynne Jones, Simon Lavis, Deepa Madhu, Jordan McErlean and Alicia Payne.

Further information on the project, its members, and current research activities is available via the project website: www.cyberterrorism-project.org.

This event was supported by:
NATO OTAN
Office of Naval Research Global Science & Technology
Swansea University Prifysgol Abertawe
Bridging the Gaps

Preface

This report contains findings from The Cyberterrorism Project's conference: A Multidisciplinary Conference on Cyberterrorism. The event was held 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. The conference built on an earlier workshop held at Swansea University in September 2012.

In due course a number of the papers from the conference will be published in the following edited collections:

- Jarvis, L., Macdonald, S. & Chen, T. (2014) *Cyberterrorism: Definition, Threat & Response.* New York: Springer.
- Jarvis, L., Macdonald, S. & Chen, T. (2014) *Terrorism Online*. Abingdon: Routledge.

This report provides summaries of each of the papers that were presented at the conference, before drawing out the key themes which emerged.

Acknowledgements

The conference organisers would like to express their gratitude to the following for their support for this conference and associated activities: the US Office of Naval Research Global Collaborative Science Programme; the NATO Public Diplomacy Programme; the EPSRC Bridging the Gaps Programme based at Swansea University and the Swansea Academy of Learning and Teaching.

Suggested Citation

Macdonald, S., Jarvis, L. & Chen T. (2013). *A Multidisciplinary Conference on Cyberterrorism: Final Report*. Cyberterrorism Project Research Report (No. 2), Swansea University. Available via: www.cyberterrorism-project.org

Table of Contents

Introduction

Cyberspace now permeates almost every aspect of our everyday lives. Today, the number of global web users is 1.7 billion: over 100 times greater than the 16 million users in 1995. By 2015 there will be more interconnected devices on the planet than humans (UK Government 2010). The pace of technological change in computing is also accelerating at an exponential rate. By 2030 the average home's computing capacity will be one million times greater than it is today (USJFC 2010).

But whilst cyberspace presents enormous opportunities, it is also a major source of critical strategic challenges. At the international level, a range of International Governmental Organisations have launched policies, strategies and other initiatives specifically on cybersecurity. These include the Commonwealth, ECOWAS, the European Council, European Union, NATO and the United Nations (for a recent example see European Commission 2013). Domestically, states and their executives have also been active in addressing these challenges. In the UK, for instance, the National Cyber Security Programme was launched in June 2011, accompanied by £650m of new investment, and the establishment of a new National Cyber Crime Unit within the National Crime Agency. The challenges confronted by these national and international bodies are multiple, evolving and frequently interconnected. Thus, although the significance of these concerns is repeatedly acknowledged (such that the UK's 2010 National Security Strategy identified cybercrime as one of the four highest priority risks to national security), the level of current and future risks from this and related cyber-activities remains relatively unknown.

Cyberspace has already been widely recognised as a new strategic environment, and will become a major front in future conflicts: irregular and traditional (USJFC 2010). In order to examine the convergence of cyberspace with one particularly prominent form of irregular warfare – terrorism – in 2011 the Cyberterrorism Project was established at Swansea University. The Project has already embarked on a number of activities, including: a global survey of the research community's understandings of cyberterrorism; the compilation of a database of existing national and international definitions of cyberterrorism; and, the creation of a database of news stories on cyberterrorism from the past five years.

In April 2013 the Cyberterrorism Project hosted an international conference in order to examine and evaluate understandings of, and responses to, the cyberterrorism threat. In keeping with the Project's aim to transcend disciplinary and jurisdictional boundaries and facilitate interaction between researchers, policymakers and practitioners, the conference was attended by a wide range of stakeholders from across Europe, the US and Australia. This report presents an overview of each of the papers presented during the conference, and draws out some of the key findings. Full versions of a number of the papers will be published in 2014 in a series of two edited collections.

References:

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission.

United Kingdom Government. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. Cm 7953. Norwich: The Stationery Office.

United States Joint Forces Command. (2010). *The Joint Operating Environment 2010*. Suffolk, VA: United States Joint Forces Command.

Panel 1: Defining Cyberterrorism (i)

Chaired by Dr Stuart Macdonald

On the Terrorist Misuse of the Internet

Dr Panayotis Yannakogeorgos (US Air Force Research Institute)

Yannakogeorgos began his talk with a hypothetical example of an insulting video of the Prophet Mohammed being picked up by terrorists and used in a protest which ended in violence. He noted that cyberspace encompasses more than the Internet alone, and includes open multifunctional networks as well as closed networks such as air traffic control systems and financial networks. The purpose of cyberspace, he argued, is to allow human operators to create effects in the real world.

Yannakogeorgos then provided the conference with a range of examples of misuses of the Internet, arguing that cyberspace is revolutionising how terrorist organisations operate. These included: (i) Communication, in terms of the possibility of spoofing or 'onion routing' – which involves masking the point of origin of a data packet; and in terms of the rise of shadow internets which are harder to police, especially with the rise of multilingual global Top-Level Domains (gTLDs) to rival .com and .co.uk; (ii) Terrorist financing and the bypassing of UNSC Resolution 1267. Botnets, Yannakogeorgos argued, could be used here for bank robberies as much as espionage and DDoS attacks; (iii) Destruction – for example, the use of viruses; and, (iv) Zero Day Exploits – those exploits not seen before and targeting vulnerabilities hitherto unrecognised. Zero Day Exploits, however, remain expensive and are therefore less common than other threats, although Stuxnet was unusual in combining four of these. Cyber-weapons and attacks, he noted, need five things: (i) Expert level programming and cryptographic skills; (ii) Detailed knowledge of industrial control systems; (iii) Masking of open and closed operating systems; (iv) Detailed knowledge of telecommunications and legal regimes; (v) Ability to maintain access, test and deploy a weapon on a closed network in order to know whether a weapon will work. Examples provided included the explosion of an industrial generator in the Aurora vulnerability and the Sayano Shushenskaya malfunction.

Yannakogeorgos concluded by arguing there are a number of ways in which terrorists could use cyberspace to multiply the face of a physical attack, and that the use of cyberspace might also be important for recruitment in addition to radicalisation.

What is Cyberterrorism? Computer Technology and Domestic Counterterrorism Laws

Keiran Hardy (University of New South Wales)

Hardy presented a paper that had been co-authored with **Professor George Williams** (University of New South Wales). To the question 'what is cyberterrorism?' Hardy argued that the legal answer is that an act only constitutes cyberterrorism if it comes under particular legal provisions. Having identified a range of potential or candidate scenarios – from attacks against critical infrastructure, to DDoS attacks, hacktivism and attacks against PayPal and websites – Hardy noted that there is no offence of cyberterrorism within his case studies of Australia, Canada, New Zealand and the UK. Thus to determine what constitutes cyberterrorism it is necessary to look at what may be designated an act of 'terrorism' under domestic law, and therefore what uses of technology would meet those requirements. Hardy argued that terrorism offences are quite unique within criminal law, and require the meeting of three conditions: (i) Intention – both to conduct the act, and to influence or intimidate the government or population; (ii) Some form of political, religious, or ideological motive or purpose; and, (iii) The bringing about of harm – for example, death or bodily injury.

Turning to the Terrorism Act 2000 of the UK, Hardy identified the pre-9/11 consolidation of prior terrorism legislation (especially in relation to Northern Ireland). This Act includes a general definition of terrorism, and the possibility of cyberterrorism was debated in Parliament at the time of its passage. In terms of this Act, terrorism may encompass both the threat of an action, and an intention to

influence government, such that attempting an act which would endanger life in order to influence a government for a political motive could fall under this. Under the UK definition death or bodily injury is not necessarily a prerequisite; an act designed to interfere with or seriously disrupt an electronic system (whatever this means) could potentially constitute terrorism. Moreover, the UK Terrorism Act includes actions in countries other than the UK – as demonstrated in *R v F* [2007] EWCA Crim 243 which involved a Libyan national accused of trying to overthrow Colonel Gaddafi before his fall from power. This case demonstrated that it is possible to commit an act of terrorism under UK law against a foreign oppressive or tyrannical regime. This very widely drafted definition of terrorism means that it would include the threat of a cyber-attack that was intended to interfere with an electronic system, and that was intended to influence a foreign government for a political motive. And, in the UK this is extended still further to include offences relating to training, support, membership, fundraising, dissemination of publications and glorification. The case of *R v Gul* [2012] EWCA Crim 280, for example, saw a sentence of 5 years imprisonment handed to an individual for posting videos on YouTube encouraging further attacks against coalition troops in Iraq.

Hardy then turned to Australia, Canada and New Zealand, noting that there is a political protest exception in Australia, while the Canadian criminal code requires that an offence must cause serious interference with essential services. In New Zealand, there are higher standards again, including that an act must be 'likely to endanger human life'.

Hardy finished by considering a more appropriate legal definition, arguing that this would retain the motive requirement, involve the inducement of terror, and refer to acts that involved interference with essential services/systems if likely to endanger life, devastate the economy or cause major environmental damage. This, Hardy argued, captures the kind of thing one has in mind if the desire is to criminalise cyberterrorism.

Cyberterrorism: A Classified Threat or an Orphan Idea?

Alexandros Kyriakidis (University of Sheffield)

Kyriakidis' paper concluded the first panel. He argued that no definition of cyberterrorism exists within international legislation, before pointing to the etymology of the term from: (i) 'Cybernetic' (coined by Norbert Wiener) from the Greek for 'the one who governs' – Kybernetes; and, (ii) Terrorism – from terrere (Latin) 'to inspire fear': a term first used in the French reign of terror.

Kyriakidis explored a range of missed opportunities to define cyberterrorism, including in: the UN's Ad Hoc Committee on Measures to Eliminate International Terrorism; the UN International Crime and Justice Research Institute (UNICRI); NATO's Cooperative Cyber Defense Center for Excellence (Estonia); G8 communiqués; the International Telecommunications Union (ITU); the International Center for Counterterrorism (a think tank which doesn't mention cyberterrorism); INTERPOL; and, EUROPOL. Kyriakidis noted that the EU Convention on Cybercrime remains the most significant international treaty in this area, but this doesn't mention cyberterrorism.

Kyriakidis then noted that no attacks to date have been confirmed as cyberterrorism. However, major alleged attacks include: (i) 'Titan Rain' (2000-2008) – a cyber-espionage case in which data was stolen from numerous companies and organisations over a number of years; (ii) Estonia (2007) – DDoS/Trojan Horse attack on media/financial websites which were defaced and shut down; (iii) Georgia – July/August 2008 – which resulted in no physical damage; and, (iv) Stuxnet (2010) – a worm only activated in specific programme configurations which was aimed at hitting specific nuclear control machinery and probably transferred via memory stick.

Kyriakidis concluded by arguing that a useful definition of cyberterrorism would be: activity done over information technology systems by governments/non-governments against individuals, creating intimidation with the ultimate goal being a political, religious or social objective.

Panel 2: Defining Cyberterrorism (ii)

Chaired by Professor Thomas Chen

Cyberterrorism as a Dependent Variable in International Law

Yaroslav Shiryaev (University of Warwick)

Shiryaev began his discussion of definitions of cyberterrorism by arguing that the definition can be deduced from written law: states, he suggested, have decided what terrorism is (and, moreover, terrorism is a crime). Shiryaev argued that there are two definitions of terrorism: archaic terrorism (which includes state terrorism); and, conventional terrorism, which refers to acts prohibited by the UN conventions and changes every time states come together. Shiryaev suggested that the two regimes/understandings are incompatible, and maintaining a distinction between them is the appropriate way to progress understanding in this area.

Cyberterrorism, he then claimed, refers to cyber-attacks that violate prohibitions enshrined in the existing legal instruments. The range of potential perpetrators include states, non-state actors, corporations and individuals.

Understanding, Locating and Constructing Cyberterrorism

Andrew Whiting (Swansea University)

Whiting presented a paper which had been co-authored with **Lella Nouri** (Swansea University) and **Dr Lee Jarvis** (Swansea University). The paper began with a brief account of the emergence of cyberterrorism as a concept in the 1980s, linking this to two prominent trends of this period. The first was a post-Cold War geopolitical reshuffle and the re-evaluation of major security threats and imaginaries at the time. The second concerned the rise of new security concerns linked to the Internet's growing significance in political, social and everyday life. Whiting then argued that although the term 'cyberterrorism' has become increasingly prominent in subsequent years, its meaning has, if anything, become more rather than less contested.

The paper then developed this account of contestability by exploring whether it is even possible to situate cyber-activities (of any kind) within a broader history of terrorism. Here, Whiting argued that terrorism, and understandings thereof, have evolved dramatically over time, so it is difficult to argue conclusively that cyber-activities cannot be incorporated within this rubric. At the same time, dominant associations of terrorism with violence and theatricality make any direct application of this language to cyber-activities difficult.

The final section of the presentation posited three competing ways to deal with the challenge of describing cyber-activities as 'terrorist'. The first was simply to abandon the concept of cyberterrorism as a misnomer: to argue, in other words, that the rubric of terrorism has no value in this concept. The second was to engage in further definitional work to clarify that to which the term 'cyberterrorism' might refer, and its association with non-cyberterrorisms. The third – the preferred route of this paper – was to eschew the question of definition altogether and approach cyberterrorism as social construction rather than brute material reality. Whiting's presentation concluded by identifying the rise of constructivist terrorist research and its implications for the study of political violence. Several concrete areas for future work were then identified, including analytical questions (how is cyberterrorism constructed?) and performative or political questions (what do constructions or representations of cyberterrorism do?).

Cyberterrorism and Moral Panics: A Reflection on the Discourse of Cyberterrorism

Dr Lorraine Bowman-Grieve (University of Lincoln)

Bowman-Grieve focused on the concept of 'moral panics' as a discursive framework through which to reflect on cyberterrorism discourses. Her paper began by introducing a recent research project that had contrasted media and academic sources on cyberterrorism, explaining the thematic analysis that had underpinned the research. This analysis moved from the identification and labelling of themes within her dataset, to interpretations of the representations of cyberterrorism therein.

Bowman-Grieve then outlined three dominant themes that had emerged from this research. These concerned, first, reflections on the risk of cyberterrorism: what is its level, what perceptions of vulnerabilities are there, and how do these change over time? Second, who is involved in cyberterrorism – which players are identified, who speaks from positions, or with voices, of authority, and how does this change over time? (Here Bowman-Grieve pointed in particular to the frequent citation of cybersecurity experts). And, third, the positing of solutions to cyberterrorism: including levels of analysis questions; the ultimate goal (reducing the threat); discussions of the costs of countering cyberterrorism (and the typical emphasis on monetary rather than social costs); and, the gradual movement away from fears of mass death to fears of financial costs. Bowman-Grieve also noted that she had been particularly interested in questions of exclusion – e.g., what is missing from discussions on cyberterrorism?

Bowman-Grieve then identified the 'moral panics' framework that structured her analysis, originally defined by Cohen in 1972. In Cohen's 2002 edition, this was described as the defining of something as a threat to societal values and interests, the nature of which is presented in a stylized and stereotypical fashion by the mass media – with rule breakers presented as deviants, for instance. (The term, she noted, is more typically employed now to refer to a range of anti-social behaviour by the media). Bowman-Grieve then turned to Jewkes' (2004) identification of the five defining features of moral panics, and their applicability to cyberterrorism. These related to the following: (i) The media turn a reasonably ordinary event into something extraordinary. So, fears around a "cyber Pearl Harbor", a digital 9/11, and descriptions of cyberterrorism as our 'single greatest threat' were identified; (ii) The media in particular set in motion a deviance amplification spiral whereby deviants are seen as a source of moral decline and social disintegration. This, Bowman-Grieve argued, was more appropriate for the earlier than later constructions of cyberterrorism; (iii) Moral panics clarify the moral boundaries of the society in which they occur, differentiating us from them and denigrating the out groups; (iv) Moral panics also occur during periods of rapid social change and anxiety. Here Bowman-Grieve pointed to the social change associated with the Internet age, and the anxiety associated with terrorism, seen now as a condition of the world; and, (v) Moral panics also tend to target young people and their behaviour, which is viewed as a barometer of societal health. Again, this had real resonance with discourses around cyberterrorism.

Bowman-Grieve concluded by citing Jewkes (ibid), who argues that the moral panics framework helps us to conceptualise "the lines of power in society and the ways in which we are manipulated into taking some things too seriously and other things not seriously enough" (p85). Further, as Altheide (2009) suggests, moral panics encapsulate the fear narrative for news purposes.

References:

Altheide, D.L. (2009). *Terror Post-9/11 and the Media*. New York: Peter Lang Publishing Inc.

Cohen, S. (2002). *Folk Devils and Moral Panics*. 3rd ed. Abingdon: Routledge.

Jewkes, Y. (2004). *Media & Crime*. London: SAGE Publications Ltd.

Panel 3: Assessing The Cyberterrorism Threat (i)

Chaired by David Mair

Cyber Threats to Critical Information Infrastructure

Dr Clay Wilson (University of Maryland University College)

Wilson's paper focused on cyber-threats to critical infrastructure. Beginning by clarifying his terms, Wilson defined infrastructures as facilities that modern society depends upon (for example, electricity) and vulnerabilities as weaknesses that threat actors can act upon. Wilson argued that distinctions between cyber-espionage/cyber-sabotage/cybercrime are blurring, and that it is hard to know if someone is 'just looking around' in one's systems or preparing for a future attack. Wilson then asked whether the cyberterrorism label depended upon: (i) Damage reaching a certain threshold; (ii) The affiliation of the threat actor; and, (iii) A combination of intent, threshold and affiliation.

The second part of the paper turned to the types of vulnerabilities which are unique to critical infrastructure facilities. These included: (i) That software updates are not often applied (in part because doing so can be expensive); (ii) That all critical infrastructure systems are becoming increasingly connected to the Internet; (iii) That intrusion detection systems and anti-virus systems can slow down critical infrastructure equipment; and, (iv) That systems with vulnerabilities can be deliberately targeted, for instance via the SHODAN search engine.

Wilson then turned to examples of cyber-attacks on industrial facilities, noting that ICS/CERT and the US Department of Homeland Security reported: nine attacks in 2009; 41 attacks in 2010; and, 198 attacks in 2011. Here Wilson discussed Aurora. Cyber-espionage was identified as a potential way of preparing for cyberterrorism – pointing to the recent Chinese stealth fighter aircraft and its similarities to other planes. Examples of cyber-espionage identified included Flame – malware which had infected computers in a number of countries, especially Iran. It had gone undetected for 4-5 years, activating microphones and video cameras, logging key strokes at keyboards and taking screen shots. Flame was followed by Stuxnet, which sabotaged nuclear centrifuges at the Natanz nuclear plant in Iran, sending false readings to facility control staff.

Wilson then turned to Zero Day Exploits, which take advantage of as yet unknown or undetected cyber facilities. As such, no defence against them exists until their discovery. Wilson noted that a market for these exists and that it is not illegal to try to sell or buy them, although global prices range to hundreds or thousands of dollars according to a report in Forbes.com. Wilson concluded by pointing to the possibility of a cyber arms race, and briefly mentioned: the emergence of related weaponry including electromagnetic pulse weapons that can burn out the circuitry of a computer by transmitting energy travelling at the speed of light; and, directed energy weapons which are microwave based and purchasable on the Internet.

Lone-Actor Terrorist Use of the Internet and Behaviour Correlates

Dr Paul Gill (University College London)

Gill described his recent collaborative research project which explored lone-actor terrorism and, within this, lone-actor terrorist use of the Internet. Gill began by arguing that literature on 'lone-wolf' (or – better – 'lone-actor') terrorism remains scarce. What there is, he suggested, focuses primarily on strategy – why lone-wolf terrorism might work in contrast to group-based terrorism. In addition, there is a lack of empirical and behavioural analysis, and much of the work is driven by very simple understandings of motive.

To address these limitations, Gill's work focused on the following two sets of questions: (i) What are the developmental pathways of lone-actor terrorism? And, are there analogous cases that can inform our understanding?; and, (ii) How do lone-actor terrorists differ? Are there identifiable categories of

lone-actor terrorists? Methodologically, the team constructed a lone-actor terrorism database, producing a code-book of 180+ potential variables which included: level of education; mental health history; age; job; and, details of the attack. Much of this data was open access and publically available because lone-wolf terrorism, to date, is rare and therefore generates much interest and news attention.

The presentation then turned to seven key findings of the research: (i) There is no uniform profile of lone-actor terrorism. For example: roughly one-half were single, one-quarter were married and one-quarter divorced; three-quarters had some university experience; 40% were unemployed; one-quarter were former military; and, 31% had mental health problems. However, 96% were male. Many lone-actors had attempted to join a terrorist group but were weeded out; (ii) In the build-up to an attack some other people generally knew about the attacker's grievance, ideology or intent; (iii) A wide range of activities and experiences preceded the plot: one-fifth were religious converts and one-half had changed address prior to the planning of the event; (iv) Many, but not all, were socially isolated: 53% were characterised thus. 37% lived alone; (v) There were distinguishable differences between sub-groups: e.g., al Qaeda associated attackers were significantly younger (average age of 25); (vi) Sudden or impulsive attacks were rare. Many attacks emerged from a gradual change of behaviours, with their origins pre-dating the actual attack by roughly two years; and, (vii) Attackers regularly engaged in a range of detectable and observable activities within wider groups.

Gill concluded by arguing that there has been no real increase in lone-actor terrorism over time and that the radicalisation process is the same as it was 15 years ago. In this sense, the Internet solely changes where the process takes place. Moreover, lone-actor use of the Internet differs. Some employ it for attack planning, others for ideological purposes and others to make contacts. Those who used the Internet to learn were primarily younger, non-American, single, student, al Qaeda-inspired, religious converts and less likely to have either military experience or a criminal record.

Cyberwarfare as a Factor in Nation-Building and Un-Building: The Case of the Assam Riots

Silviu Petre (National School of Political Science and Public Administration, Bucharest)

Petre focused on the Assam riots of 2012 in North East India, and the impact of the Internet on these. Petre explored notions of the digital divide and the centrality of warfare to state formation (using the work of sociologist Charles Tilly who argued 'war made the state and the state made war'). In his discussion, Petre pointed to two paradoxes within the Indian cyberspace. First, was the educational/institutional paradox: given the disconnect between India's IT expertise and manpower on the one hand and the limited electronic infrastructure in India and its widespread poverty on the other. The second paradox concerned India's relationship with other South Asian countries, including Pakistan. In the case study discussed, Petre explored the alleged Pakistani cyber-attack in the aftermath of the Assam Riots, in which thousands of people received hate emails and phone messages ostensibly aimed at the inflammation of inter-communal violence in an area containing 8% of India's total landmass, and 3.8% of the state's population.

Panel 4: Assessing The Cyberterrorism Threat (ii)

Chaired by Lella Nouri

Hybrid Threats, Cyber Threats and Asymmetric Threats – New Challenges to Peace and Security

Dr Sascha-Dominik Bachmann (University of Lincoln) & **Dr Håkan Gunneriusson** (National Swedish Defence College)

Bachmann and Gunneriusson began panel four with a discussion of hybrid, cyber and asymmetric threats as potential new challenges to international peace and security, requiring a new form of holistic response from law enforcement counter cyber strategies to kinetic responses. The term 'hybrid threats' was worked on by NATO between 2010 and 2012, and then subsequently abandoned because of a lack of funding. It refers to multi-modal, low intensity, kinetic and non-kinetic threats to international peace and security – including, for instance, cyber, piracy, and global terrorism. Bachmann and Gunneriusson pointed out that states, or even IGOs such as NATO, currently lack the capacity to 'go it alone' and deal with cybersecurity threats unilaterally.

Bachmann and Gunneriusson then pointed to the different types of cybersecurity threats that exist in the twenty-first century: from hacktivism, crime and sabotage through to terrorism and beyond. Social media, they noted, is part of the cyber sphere, and implicated in previous attacks such as in Mumbai. Here, the main issue is the mass availability of messages and communication. Turning next to the connection between war and cyber, Bachmann and Gunneriusson questioned whether a prolonged sustained cyber-attack could qualify as an armed attack pointing out that under international law a state can act in self-defence under Article 2(4) of the UN Charter when faced with a threat from another state. They noted that there also exist collective defence principles, such as Article V of NATO's charter. A second question asked was 'what happens if a cyber-attack is completely dissociated from conventional attacks (for example, Stuxnet)'? Does this constitute an act of war? Bachmann and Gunneriusson argued that it does – if the impact is there – under Article 51 of the UN Charter regarding self-defence. At the same time, this is debatable in practice as there is currently no case law on this. Force is legitimate, then, when it is either: (i) Exercised in self-defence; (ii) Authorised by Article 51; or, (iii) Authorised by 'humanitarian catastrophe' concerns as in R2P (although this is more debatable). Bachmann and Gunneriusson concluded by arguing that, in a sense, 'the future is already here', albeit that it is not yet evenly distributed. Cyber-attacks, they suggested, will take place.

Three Arguments Against Cyberterrorism: Technological Complexity; the Image Factor; and, the Accident Issue

Dr Maura Conway (Dublin City University)

Conway's paper concentrated on three main arguments against the likelihood of cyberterrorism occurring. These concerned: (i) Technological complexity; (ii) The image factor; and, (iii) The accident issue. Conway began by distinguishing between cyberterrorism and terrorist uses of the Internet, arguing it is important to keep these two phenomena analytically separate. She then noted that whilst cybersecurity is important, terrorists therein are not the major threat. She emphasised that her focus is what is likely from a terrorism perspective, rather than what is possible from a technological perspective. In this sense, her paper represents something of a corrective of the dominant focus of literature in this area. In terms of definitions, Conway noted that she was following Dorothy Denning's understanding of cyberterrorism, and focusing primarily here on 'Jihadis'. Conway then turned to her three main arguments.

First, technological complexity. Jihadi knowledge of IT or cyber is not, she noted, superior to the ordinary public: good or convincing online propagandistic content does not equate to a capacity to engage in cyberterrorism. Conway here referenced a 2007 survey of Jihadis that found that only eight out of 178 had training in computing. On top of this, she noted that real world attacks are difficult

enough and often are unsuccessful (e.g., the Glasgow attack), and that the possibility of terrorist organisations hiring hackers is limited as this would be operationally risky raising the possibility of infiltration of the group from outside. There would also be the challenge of the terrorist group gauging the competence of the hired hacker.

Turning, finally, to the possibility of crowd sourcing as a response to these types of challenge, Conway argued that the problem with this is that the author loses control over the means of the attack – rendering crowd-sourcing, perhaps, less desirable.

Second, the image factor argument. This built on the twentieth century experience of spectacular moving images constituting an important part of terrorist attacks – 'performance violence' – not least regarding 9/11. In terms of cyberterrorism, many of the hypothesised attack scenarios are unlikely to replicate this (such as the contamination of water supplies or the shutting down of the power grid) and therefore are likely to be less appealing than their more dramatic offline counterparts.

Third, the accident issue. This develops this understanding of terrorism as a form of violent communication, noting that a terrorist attack that cannot be attributed doesn't make for a very good terrorist attack. Terrorists don't, Conway argued, tend to want deniability. They want to claim responsibility for their attacks, yet we don't know the true source of events like NIMDA and Code Red.

Conway concluded by pointing to the al Qassam Cyber Fighter group associated with al Qaeda that has recently committed a range of attacks against US banks. The problem, she noted, is that very few people have heard about this group (#opisrael offered a related example). Cyber-based activities, then, don't tend to work as terrorism, and the dominance of debate in this area by a technological rather than a terrorism perspective has skewed assessment of risk scenarios. From a terrorism perspective, Conway argued, the costs largely outweigh the publicity benefits.

Putting the 'Cyber' into Cyberterrorism: Re-Reading Technological Risk in a Hyperconnected World

Dr Michael McGuire (University of Surrey)

McGuire focused his talk on an appeal for better understanding of what 'cyber' is and its importance in discussions of cyberterrorism and cybersecurity. He began with an example of the Roman Cursus Publicus. This was the original Roman postal system, which from its outset was plagued by all sorts of security fears – around criminality, but also illicit communication involved in radicalising potential subversive elements. To combat these fears, the Romans replaced relay messages with single carriers to improve security, the corollary of which was a huge reduction in the efficiency of the system. McGuire argued that the Cursus Publicus was clearly a technology (although never defined in that way) and therefore has parallels with the telegraph system of the nineteenth century or the printing networks of the eighteenth century. What is striking is that we don't think of any of these things as technologies that facilitated terrorism. Why, then, do we think of cyber in this way?

McGuire then noted that the idea of 'cyberspace' is hugely problematic, before introducing different approaches to risk assessment (in terms of category questions and harm questions). For McGuire, the term 'cyber' is a red herring for it implies a unique domain of activity. McGuire argues, therefore, that we should be looking at ICT – without which there is no cyber. The presentation then turned to three different basic models of causality that underlie assumptions that IT causes terrorism: (i) ICT being used for communications and radicalisation; (ii) ICT being used for attacks on networks; and, (iii) ICT being used for wider forms of physical harm. However, causation typically denotes two things: that C (the cause) makes a difference to E (the effect); and, that there is an underlying mechanism which explains how/why C makes a difference to E. McGuire argued that neither of these are clear in scenarios (i) or (iii).

McGuire then suggested that how technology causes something is difficult to explain. Three different models of technology are: (i) The neutral model: agent + (inert) tool = outcome (instrumentalism); (ii)

The addition model: agent + (causally active) tool = outcome (the idea of enablement); and, (iii) The fusion model: agent plus tool form a new kind of causal agent (as in B-52s do not fly, the US Air Force flies). The problem with instrumentalism is that it makes terms such as cyberterrorism vacuous (the cyber has no explanatory purchase). It also creates a façade of normative inertness. The enablement model has problems, too, in that it frequently becomes circular or a tautology failing to capture causality. In response, McGuire offered a 'post-human' view, where technology and human agency create something new: an existential, prosthetic view of human/technology continuities. Technologies (following McLuhan and Freud) function here as extensions of our physical and nervous systems – they extend us.

In terms of assessing the risk of cyberterrorism, this post-human understanding helps to move us beyond technological fetishism, and taps into the notion of the contemporary world as one of hyperconnection, whereby: connections are always on; more things than ever are connected; accessibility is always available; interfaces are invisible; and, information is continuously recorded. As such, interaction can happen with anyone, anywhere and at any time. The impacts of hyperconnection include enhanced targeting possibilities, especially businesses and business systems.

Dr Strangeweb: Or How We Stopped Worrying and Learned to Love Cyberwar

Professor Michael Stohl (University of California, Santa Barbara)

Stohl began his paper by referencing a 1985 talk he had given on terrorism, state terrorism and state-sponsored terrorism. In that talk he had focused on the superpowers, arguing that doing so would tell us more about decisions to deploy terrorism than the unknown decision-making processes of other states. This was particularly so given that resources in the global system were concentrated in the hands of the superpowers, and the bipolarity framework within which international terrorism occurs takes its norms from the most powerful actors in the system. Superpowers, he argued, had the greatest capacity and interest in controlling the use of terrorism.

Stohl argued that a meaningful parallel could be drawn between discussions about states and state terrorism on the one hand, and cyberterrorism/cyberwar on the other. He argued that, while the potential of cyberterrorism does continue to exist, no electronic Pearl Harbours or Hurricane Katrinas have yet occurred.

Stohl then pointed to the ways in which states have increased resources within their own cyberwar capabilities and encouraged private sector actors to do so too. He then turned to relevant contemporary events including the 2007 attack on Estonia which did not generate much public anxiety (as the Daily Mail put it, 'No one died'), the 2008 Russian/Georgian conventional war in which media and public interest waned almost immediately, the 2012 claim of responsibility for the Stuxnet worm by President Obama, and the 2012 identification of Red October which may have been more dangerous than originally reported.

The US military has been concerned about cyberwar for a long time. The movement from C3 to C4ISTAR is evidence of a dramatic expansion of cyber components within the US. The first US cyber strategy was published in 2003, and the budget has increased annually since. May 2010 saw the creation of the US Cyber command.

Moreover, the US has been explicit on the need for offensive capabilities in this domain, and has formally recognised cyberspace as a new environment for warfare. Stuxnet is much more ambiguous than any weapons ever created by anyone else – state or non-state – and there is a continuing increase of budgetary resources here. Importantly, no-one can really match this level of investment and resources, and the US is clearly making its effects well known, although China and Russia have also made significant investments, especially in relation to cyber-espionage.

Returning to the state terrorism/cyberterrorism parallel, Stohl argued that both demonstrate that states undermine the norms that could be used to confront the threats that they are wary about.

Panel 5: Responding To Cyberterrorism (i)

Chaired by Andrew Whiting

How Feasible is US-EU Collaboration in Countering Cyberterrorism?

Eva Nagyfejeo (University of Warwick)

Nagyfejeo's paper focused on transatlantic cooperation in cybersecurity and cybercrime. Beginning with the attack on Estonia – one of the most wired countries in the world – that followed the removal of a WW2 monument, Nagyfejeo argued that 3 lessons had been learned: (i) That national police forces and legal systems struggle to keep up with developments; (ii) That the core overarching problem of developing effective cyber defence capabilities still lies in the prevalence of national interests among Member States; and, (iii) That a more effective and quicker response to cyber-threats is needed.

Nagyfejeo then turned to three achievements: the Tallinn Manual (2013) initiated by NATO's Cyber Defence Centre of Excellence (which identifies 95 black letter rules that represent restatements of the law applied in the cyber context); the 2012 Chicago Summit Declaration (helped to bring all NATO bodies under centralized cyber protection and created a rapid reaction team to assist Member States when they are suffering from significant cyber-attack); and, the 2011 Cyber Defence Policy (confirms that cyber intrusions at the Member State level must be handled politically, rather than militarily, under Article 5). On transatlantic cooperation in cybersecurity, Nagyfejeo argued that the US had taken a primarily 'laissez faire'/voluntary approach (partly due to fears of over-regulation by US businesses), yet is ahead of Europe in integrating military cybersecurity into its foreign and security policy. The EU, in contrast, has taken a more regulatory approach, including with the EU Cyber Security Strategy of 2013 and its accompanying Directive which made compulsory the reporting of cyber incidents across different sectors. She argued that this raises the question of whether the US needs more regulation. Regarding which legal framework the transatlantic community can apply in any cyber-threat scenario, the Budapest Convention on Cybercrime remains the only legal instrument – signed and ratified by 23 countries.

Nagyfejeo pointed to numerous challenges for cooperation in the future, including: (i) Different strategic and security cultures in the US and EU – while the EU has a long history of dealing with domestic terrorism, it is less equipped in term of fighting cybercrime than the US; (ii) Different levels of cybersecurity preparedness – she argued that the US intends to militarise cyberspace for its own national interests, while the EU does not talk about warfare nor does it have the defence element in its strategies. Rather, it focuses more on building competences through international collaboration; (iii) The existence of ambiguous definitions in the cyber domain; and (iv) Problems of law enforcement cooperation.

Nagyfejeo finished by pointing to the paradox of cybersecurity. The growing complexity of the Internet leads to its increasing importance in contemporary life. This leads to a higher number of stakeholders, and concomitantly a higher level of vulnerability. This renders the Internet more difficult to regulate, and therefore more complex to deal with, and the cycle continues.

The Use of Force as a Response to Cyberterrorism

Dr Irene Couzigou (University of Aberdeen)

Couzigou focused on the use of force as a response to cyberterrorism. She began by noting that international law has a prohibition on the use of force between states: Article 2(4) of the UN Charter states that all Member States shall refrain from the threat or use of force (a provision of international customary law). The question, then, is whether cyberterrorist attacks can be seen as an act of armed force using either an instrument based approach or a consequence based approach.

Couzigou argued that cyber-attacks that cause physical damage to tangible property or injury or death to human beings can reasonably be characterised as a use of force. Yet, a cyber-attack on a state's financial infrastructure much more closely resembles economic coercion than traditional armed force.

Couzigou then turned to the two well-recognised exceptions to the prohibition on the use of force in international law. First is where authority is given by the UN Security Council under threats to peace (Articles 39 and 42 of the UN Charter). A cyber-attack that is a serious use of armed force could qualify as a threat to peace here. However, in international law one cannot rely on the Security Council as the UNSC is a political actor, not obliged to act, subject to the veto powers of the P5, and may be insufficiently quick in responding.

The second exception is under the right to self-defence, guaranteed by Article 51 of the UN Charter with reference to armed attacks. One difficulty is that these are not really defined by the International Court of Justice, which identified them as 'the most grave forms of the use of force' performed with the intention of harming (reference was given here to the definition of aggression given by the UN General Assembly). Can cyberterrorist attacks count as an armed attack? Yes, given the conditions outlined at the start of the paper. Then, the issue turns to state involvement for, as Couzigou concluded, Article 51 of the UN Charter only recognises the right to self-defence against state actors, not non-state actors. Her argument is that this should also be allowed in reference to non-state actors.

Panel 6: Responding To Cyberterrorism (ii)

Chaired by Wynne Jones

Cyberterrorism and the Reconstruction of the Customary Rule about Terrorism of the Special Tribunal for Lebanon

Dr Nadina Foggetti (University of Bari)

Foggetti focused on cyberterrorism and the reconstruction of the customary rule regarding terrorism. In her introduction, Foggetti began by pointing to the UN General Assembly Resolution 66/178 of 2011 which reaffirmed the mandate of UNODC to continue to develop specialised legal knowledge in the area of cyberterrorism. She then turned to a range of definitions from academia to the FBI and NATO. She argued that these definitions share the following elements: (i) a motive element – a political or ideological goal; and (ii) an intention to generate a public danger or fear.

Foggetti then turned to the Special Tribunal for Lebanon which was established by a Security Council Resolution under Chapter VII of the UN Charter (the Lebanese government had previously failed to ratify an agreement with the UN). The Tribunal's jurisdiction covers the prosecution of those responsible for the assassination of Prime Minister Rafic Hariri on 14 February 2005. Significantly, the Special Tribunal does not apply international (criminal) law, but rather national law. It is also the first time that an UN-based international criminal court has tried a 'terrorist' crime committed against a specific person.

Preventing Acts of Cyberterrorism: The Criminalisation of Preparatory Activities

Dr Stuart Macdonald (Swansea University)

Macdonald began by outlining the wide range of precursor criminal offences (offences which apply to preparatory activity prior to any attempt to commit a planned attack) which are available in terrorism cases, and discussed whether it is possible to justify these offences in terms of criminalisation theory. Focussing on the harm principle, he explained that precursor offences may be justified if the defendant had some normative involvement in the feared eventual attack. He argued that some of the existing precursor offences exceed this constraint, since they can apply to individuals who engaged in wholly innocent conduct and individuals with no terrorist connections or intentions.

In the second half of his presentation Macdonald focussed on whether precursor offences should be available in cases where the feared eventual attack is a cyber-attack (as opposed to a traditional physical terrorist attack). He explained that at present in the UK the full range of precursor offences is available in any case where a terrorist launches an attack which seriously interferes with, or causes serious disruption to, an electronic system (section 1(2)(e) of the Terrorism Act 2000). He argued that this is overly broad. Whilst the availability of the precursor offences may be justifiable in cases where interference with an electronic system will cause enormous economic or environmental harm, the preventative rationale which applies in cases involving serious violence against people or property is far less potent where, for example, the effect of an attack is to render a website unavailable for a number of days.

Macdonald concluded by saying that the reason we place such importance on prosecuting suspected terrorists is the criminal law's moral authority and fairness. Overly broad precursor offences thus risk undermining the reasons we insist on prosecution in the first place.

Cyberterrorism and Deterrence

Dr Patrick Bishop (Swansea University)

Bishop offered a theoretical analysis of the extent to which deterrence orientated criminal law and enforcement might be effective in the context of cyberterrorism. His starting point was Becker's deterrence calculus which, in rudimentary terms, postulates that compliance will be ensured where the expected penalty associated with a criminal act, discounted by the probability of apprehension, exceeds the likely gains from illegal activity: $U < pD$ – where U is the profit/benefit from an offending activity, D is the cost to the offender of being apprehended and p is the probability of being apprehended (Ogus & Abbot 2002). Bishop then argued that the extent to which the criminal law is capable of deterring illegal conduct is a highly contested issue; a survey of the academic literature reveals considerable scepticism about the ability to deter crime through the manipulation of law enforcement practices and criminal sanctions. Indeed, it is possible to argue that is better to incentivise non-terrorist activity than to try to deter would-be terrorists.

Bishop then unpacked the deterrence calculus and a number of its neoclassical economic assumptions, specifically, that members of the target audience behave as rational profit maximisers and are able to obtain sufficient information to conduct an accurate assessment of the risks of criminal activity. Further, academic discourse is replete with assertions to the effect that the potential deterrent effect of the criminal law is bolstered where the offending activity is also subjected to community censure. Thus, he argued, the conditions which must exist for effective deterrence are seldom, if ever, present in the context of terrorism in general and cyberterrorism in particular. Further, the mainstream criminological viewpoint is that increasing the probability of apprehension (as opposed to increasing the severity of sanction) is a more efficacious method of enhancing deterrence. In the specific context of a cyber-attack, the inherent nature of cyberspace (anonymity, jurisdictional complexity, etc.) is such that criminal investigation and enforcement policies designed to increase the probability of apprehension are problematic; even if successful, such measures would be expensive and possibly overly draconian, thereby acting as a further inducement to engage in terrorist activity.

Bishop argued that the extent to which the criminal law and criminal enforcement is able to achieve a deterrent effect in the context of cyberterrorism is uncertain at best. In addition, as a policy response, the resources needed to bolster the deterrent effect of legal sanctions may be better targeted at technological innovations designed to maintain the situation which produces (from the terrorist's viewpoint) an unfavourable cost-benefit ratio for any proposed cyber-attack.

References:

Ogus, A. & Abbot, C. (2002). 'Sanctions for Pollution: Do We Have the Right Regime?' *Journal of Environmental Law*. 14(3): 283–98

Panel 7: Responding To Cyberterrorism (iii)

Chaired by Simon Lavis

The Ethical Questions of Countering Cyberterrorism

Dr Ross Bellaby (University of Sheffield)

Bellaby explained that the growth in the use of the Internet presents both opportunities and challenges. Whilst it gives terrorists new tools for causing harm and damage, it also brings the ability to detect, locate and prevent (cyber)terrorist threats. As such, there is considerable impetus for the intelligence community to gain a footing in the cyberworld, resulting in a great turn towards new cyber-based methodologies and technologies such as data-mining (involving the trawling of databases for personal information and the centralisation of such information as DNA, money, location and biographic data) and dataveillance (including individuals' web logs and IP addresses).

Bellaby's focus was the ethical concerns for the use of such technologies. He began by introducing the concepts of privacy (including the distinction between "Privacy as boundaries" and "Privacy as control"), autonomy and social cohesion. He then outlined different types of searches (targeted searches about individuals, event driven searches, pattern based searches and website monitoring) and different types of information (traffic data about the location of the device which sent or received a communication, use data such as phone records, and subscriber information about who has accessed what online). Bellaby then identified some of the key ethical problems, in terms of privacy and social cohesion. He pointed to the danger of database overrepresentation and marginalisation, and argued that self-monitoring increases with increased privacy expectations.

Finally, Bellaby concluded by looking at possible justifications for just surveillance. He highlighted the notions of just cause and legitimate authority, and emphasised the importance of discriminating between legitimate and illegitimate targets.

Of Citadels and Sentinels: State Strategies for Contesting Cyberterror

Dr Tim Legrand (Griffith University Queensland)

Legrand focused his talk on the spectre of cyberterrorism and the spectrum of catastrophic scenarios it portends for the United Kingdom. He began by noting that significant elements of state administration, national critical infrastructure, corporate enterprise and social, financial and economic systems are all increasingly interdependent and, moreover, increasingly nested within vulnerable digital ecosystems. On a daily basis, state officials detect cyber-intrusions growing in frequency and sophistication from antagonistic governments and politically-motivated or criminal groups. The stakes for public policy, the private sector and society at large have never been higher.

Legrand then suggested that governments worldwide now face the task of creating or adapting state institutions to engage with rapidly evolving, elusive and recalcitrant cyber-threats that have the potential to cause harm to life, limb or livelihood. Identifying the principal UK and international institutions mandated to address cyberterrorism, Legrand explored the series of complex policy problems that continue to confound government agencies and corporate actors, particularly since the majority of critical infrastructure is owned and operated by the private sector. Principally, he focused upon the conflict that has arisen between the protection of the public interest and the pursuit of corporate goals in cybersecurity. Government's capacity to remedy this conflict is limited and thus far confined to soft regulatory approaches aimed at coordinating the sharing of information on threat and protection. Yet at the same time, government has sought to bring its own core services – defence, intelligence, communications, etc. – within a walled-garden to share in common protection rendered by specialized government agencies. Here he contended that the scale and pace of technological change will continue to outstrip the capacity of orthodox (inflexible) political institutions to meet emerging cybersecurity threats. State institutions generally, and those engaged with cyber issues

specifically, will need to adopt a pliant policy platform to adequately contest and resist emerging hostile cyber-threats.

Responses to Cyber-Attacks

Dr Gil Ad Ariely (Interdisciplinary Center Herzliya, Israel)

Ariely began by noting the definitional problems surrounding cyberterrorism. He explained that these are in part due to the definitional issues surrounding terrorism, but also because the nature of terrorists' use of the Internet, cyberspace and IT is less well defined and delineated. The basic approach to cyberterrorism as the convergence of cyberspace and terrorism covers not just cyberterrorist attacks but also the use of cyberspace for terrorist activities. In terms of responding to cyberterrorism it is futile, he argued, to try and maintain a distinction between cyberterrorist attacks and online terrorist activities.

Ariely then argued that the challenges of cyberterrorism go beyond anonymity and attribution. IT security is increasingly outsourced, to commercial centres of excellence operating within boundaries, jurisdictions and legal frameworks that differ for each organisation. This can be exploited by adversaries that are aware of these limitations.

Ariely then discussed cyber deterrence. Anonymity, attribution and the lack of a specific physical location make retaliation almost impossible, so the base for any deterrence fades away. Moreover, cyberterrorism can be practised from relatively safe environments, so even if anonymity is breached the cyberterrorist may sit beyond the reach of any legal framework that defines his conduct as illegal. Ariely suggested an alternative approach. Exposing hackers as cyberterrorists may immediately make them a target themselves. This could at least raise the entry barrier, prompting the more novice actors or those that are just mobilized hacktivists or radicalized individuals to think twice.

Finally, Ariely emphasised that responses to cyberterrorism cannot stand alone. They must form part of broader counterterrorism policies. Existing frameworks for cooperation in countering terrorism must be adapted to include cyberterror.

Findings

Several recurrent themes emerge from the preceding summary of the seven panels:

- It is clear that cyberspace opens considerable potential opportunities for terrorist activities, including communication, fund-raising and attacks. It remains an open question whether terrorist uses of the Internet constitute an evolutionary or revolutionary dynamic. This question hinges, in part, on one's view of how the Internet differs to earlier technologies.
- 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 unproved, 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: 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.

These conclusions show clearly the considerable scope that exists for further multidisciplinary research into the issues surrounding responses to cyberterrorism, the threat that it poses and the concept itself.

Conclusion

We were pleased to welcome to the conference delegates from a number of countries across Europe, as well as Australia and the United States, and a mixture of researchers, policymakers and front-line professionals. This reflected the aims of the Cyberterrorism Project to facilitate global networking activities and engage with the full range of stakeholders. Most of all, we were delighted that delegates had such a diverse range of disciplinary backgrounds, including law, politics, IR, economics, criminology, psychology, computer science and engineering. This ensured the "multidisciplinary and pluralist context" for the discussions which took place during the conference that we believe is essential for research into cyberterrorism. With multidisciplinary research there can be a danger that discussions become fragmented and divided along disciplinary boundaries. Thanks to the quality of the papers presented by our speakers, this was not our experience. The clarity and accessibility of their presentations generated numerous stimulating discussions and important and insightful conclusions that spoke to the other attendees regardless of disciplinary background.

Appendix: List of Delegates

Suliman Alharbi, Swansea University
Dr Gil Ad Ariely, Interdisciplinary Center Herzliya, Israel
Dr Sascha-Dominik Bachmann, University of Lincoln
Roy Barrington, Thames Valley Police
Dr Ross Bellaby, University of Sheffield
Dr Patrick Bishop, Swansea University
Dr Lorraine Bowman-Grieve, University of Lincoln
Lord Carlile of Berriew QC, former Independent Reviewer of Terrorism Legislation
Professor Thomas Chen, Swansea University
Dr Maura Conway, Dublin City University
Dr Irene Couzigou, University of Aberdeen
Wim de Koning, Leiden University
Adam Drew, Royal Holloway, University of London
Dr Nadina Foggetti, University of Bari
Fiona Gaskell, Specialist Operations, Her Majesty's Inspectorate of Constabularies
Dr Paul Gill, University College London
Dr Håkan Gunneriusson, National Swedish Defence College
Joanna Halbert, Swansea University
Gavin Hall, Coventry University
Keiran Hardy, University of New South Wales
Dr Lee Jarvis, Swansea University
Peter Jones, Deputy Director for Online Services & Infrastructure, Welsh Government
Wynne Jones, Swansea University
Alexandros Kyriakidis, University of Sheffield
John Lamb, Birmingham City University
Simon Lavis, Swansea University
Dr Phil Legg, University of Oxford
Dr Tim Legrand, Griffith University Queensland
Dr Stuart Macdonald, Swansea University
Deepa Madhu, Swansea University
David Mair, Swansea University
Eamonn Maguire, University of Oxford
Dr James Maw, Swansea University
Jordan McErlean, Swansea University
Dr Michael McGuire, University of Surrey
Eva Nagyfejeo, University of Warwick
Lella Nouri, Swansea University
Silviu Petre, National School of Political Science and Public Administration, Bucharest
Duncan Pugh, Thames Valley Police
Iestyn Pugh, Trust and Security Manager, Welsh Government
Yaroslav Shiryaev, University of Warwick
Theodoros Spyridopoulos, University of Bristol
Professor Michael Stohl, University of California, Santa Barbara
Alexandros Tarkas, Defense & Diplomacy Monthly
Chrysoula Toufexi, Newcastle University
Andrew Whiting, Swansea University
Professor Clay Wilson, University of Maryland University College
Dr Panayotis Yannakogeorgos, US Air Force Research Institute

the cyberterrorism project

Contact Details

ctproject@swansea.ac.uk

www.cyberterrorism-project.org

www.facebook.com/CyberterrorismProject

@CTP_Swansea

Project Directors

Professor Thomas Chen
College of Engineering

t.m.chen@swansea.ac.uk
@TomChenTwt

Professor Thomas Chen is an expert in computer and network security. His previous research projects have explored Internet security, intrusion detection, attack modelling, malicious software and cybercrime, with support from various US agencies and companies. He is co-editor of *Broadband Mobile Multimedia: Techniques and Applications* (2008) and *Mathematical Foundations for Signal Processing, Communications, and Networking* (2011), co-author of *ATM Switching Systems* (1995), and has published papers in a number of IEEE journals including *IEEE Computer, IEEE Security and Privacy, IEEE Internet Computing,* and *IEEE Transactions on Smart Grid*.

Dr Lee Jarvis
Department of Political and Cultural Studies

l.jarvis@swansea.ac.uk
@LeeJarvisPols

Dr Lee Jarvis' research focuses on elite and non-elite understandings of terrorism, as well as the social and political impacts of counter-terrorism powers. His work is either published or forthcoming in journals including *Security Dialogue*, *Political Studies*, *International Relations*, *Critical Studies on Terrorism*, and *Citizenship Studies*. He is author of *Times of Terror: Discourse, Temporality and the War on Terror* (2009), and co-author of *Terrorism: A Critical Introduction* (2011). His most recent research project is the ESRC-funded: *Anti-Terrorism, Citizenship and Security in the UK*.

Dr Stuart Macdonald
School of Law

s.macdonald@swansea.ac.uk
@CTProject_SM

Dr Stuart Macdonald researches criminal law and criminal justice. He has written a number of articles examining frameworks for analysing and evaluating anti-terrorism policies and legislation. These have been published in leading international journals, including the *Sydney Law Review* and the *Cornell Journal of Law and Public Policy*. He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney. His recent project on security and liberty was funded by the British Academy.