Terrorists' Use of the Internet: A Symposium

Final Report

June 2014

the cyberterrorism project

About the Project

The Cyberterrorism Project is an international, interdisciplinary research network that was established by academics working across a number of fields including Engineering, Law and Politics in 2011. 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.

Recent activities of the Cyberterrorism Project include hosting conferences in Birmingham (UK) and Swansea (UK), conducting a global survey of researchers, and constructing a database of international definitions of cyberterrorism. Findings from these activities have been published in top international journals including *Terrorism and Political Violence, Studies in Conflict and Terrorism,* and *Perspectives on Terrorism,* and in books including *Cyberterrorism: Understanding, Assessment and Response* (Springer, 2014) and *Terrorism Online: Politics, Law and Technology* (Routledge, forthcoming). Further information on the project, its members, and ongoing research activities is available via the project website: www.cyberterrorism-project.org.

For membership and media enquiries please contact the project directors (p. 25).

This event was supported by:
Swansea University Prifysgol Abertawe
Curtin University
Office of Naval Research Global Science & Technology

Preface

This report contains findings from the Cyberterrorism Project's symposium on terrorists' use of the Internet. The event was hosted by Swansea University, UK, on 5-6 June 2014. 43 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.

This report provides summaries of each of the papers presented at the symposium, drawing out the key themes which emerged.

Acknowledgements

We would like to thank the US Office of Naval Research Global, Swansea University and Curtin University for supporting the symposium. We would also like to thank Simon Lavis for his help during the symposium and in the design of this report, and Verity Cannell, Julia Carroll, Kirstie Dunseath, Louise Edgington and Guy Szablewski for assisting with the hosting and promotion of the event.

Suggested Citation

Macdonald, S., Aly, A., Chen, T., Jarvis, L., Mair, D., Nouri, L & Whiting, A. (2014). *Terrorists' Use of the Internet: A Symposium – Final Report*. Cyberterrorism Project Research Report (No. 4). Available via: www.cyberterrorism-project.org

Table of Contents

Introduction

Cyberspace is now widely recognised as a key strategic environment with governments, businesses and citizens facing a range of cyber threats from cybercrime and disruptive network attacks to emerging forms of destructive cyber arms. The significance of these threats will continue to rise in the coming years as more and more aspects of public and private life migrate online and dependence upon the Internet and digital networks grows still further with networked healthcare and growing numbers of smart objects such as vehicles and home appliances. The development of virtual currencies and emerging technologies such as three-dimensional printing will intensify cyber threat levels still further.

As the security landscape evolves, so too will the terrorist threat. Terrorist organisations have already expressed an interest in developing offensive cyber capabilities. The potential for malware to be used strategically as a weapon was illustrated by Stuxnet. Whilst a very high level of sophistication and resources were needed to develop Stuxnet, malware for sabotage may be expected to become more prevalent and "mainstream" in the next five to ten years as the required knowledge and skills to mount such an attack become more widespread. Indeed, the FBI has predicted that terrorists will exploit this emerging capability for network-based attack by developing or hiring hackers for the purpose of complementing large conventional attacks with cyberattacks.

Whilst terrorists launching cyberattacks potentially poses a future threat, they already use the Internet for a range of other activities. These include: planning; communication; propaganda; recruitment; training; and, fundraising. This symposium brought together a range of experts from different disciplines (across the physical and social sciences) and different jurisdictions (from across Europe, Canada and Australia) in order to:

- Explore different forms of online terrorist activity;
- Evaluate legislative and policy responses to terrorists' online activities in terms of their impact on democracy, liberty and the rule of law; and
- Explore the opportunities that the Internet provides for intelligence and enforcement agencies, not only for surveillance and intelligence but also the construction and promotion of counter narratives and other strategic communications.

The symposium consisted of a total of six panels. The first two panels examined a wide range of terrorists' online activities, including propaganda, radicalisation and finance. The third and fourth panels focussed specifically on the possibility of terrorists launching cyberattacks and the discourse surrounding this possibility. The final two panels then concentrated on issues of response, including cyber surveillance, legal regulation of intelligence and investigation and the role of the private sector.

This report presents an overview of each of the papers presented during the symposium, and draws out some of the key findings. A number of the papers may also be viewed in full via the project website: www.cyberterrorism-project.org.

Panel one

'Electronic Jihad': The Internet as Al-Qaeda's Catalyst for Global Terror

Prof Martin Rudner, Carleton University

Rudner's paper presented the al-Qaeda twenty year strategic plan (2001- 2020) with a focus on the prominent use of the Internet within this strategy. al-Qaeda has deemed the Internet 'a great medium for spreading the call of jihad and following the news of the Mujahideen (Islamic warriors)'. Rudner's paper covered the strategic and operative elements of 'electronic jihad'.

Rudner began by discussing the al-Qaeda strategy of electronic jihad which seeks to exploit the strategic capabilities of the Internet to foster a radical jihadist counter culture that challenges the traditional authority of established religious scholars in Muslim communities and those in the Western diaspora. Rudner highlighted the strategic elements of 'electronic jihad' which included incitement to and support for violence, dissemination of propaganda (webcasting news, glorification of martyrs, translating propaganda material, publishing online magazines), and delivering military training and instructions on computer security.

Rudner went on to discuss the relative advantages of the Internet for jihadist groups. The Internet offers such groups access to a global 'virtual Ummah' to whom they can disseminate their version of a homogenized jihadist culture. As such, jihadist websites function as online libraries, platforms for extremist preachers and forums for radical discourses — these are the operative elements of electronic jihad.

The messages embedded within jihadist websites configure the radical Islamist doctrine for Muslim diaspora communities attempting to subvert Muslim communities in Western democracies, promote support for violence and offer theological justifications for terrorism. Such websites not only promote the use of violence, they also provide training and instruction in carrying out acts of violence, promote direct involvement and encourage personal engagement with the jihadist cause. Thus, Internet activities span the full gamut of activity from incitement to recruitment and training.

In closing Rudner quoted the current leader and commander ("Emir") of al-Qaeda, Dr Ayman al Zawahiri, whose words serve as a caveat on the potential destructive capacity of electronic jihad that projects radical Islamism to globally dispersed communities while mobilizing prospective followers to the cause.

#Westgate: A Case Study

David Mair, Swansea University

Mair's paper presented the initial findings from an analysis of 265 Tweets sent from accounts claiming to be directly linked to al-Shabaab. These accounts operated during the Westgate shopping mall terrorist attack in Nairobi, Kenya in September 2013. In total, seven Twitter accounts were identified which tweeted between one and 98 times over the course of their lifetime.

Mair began with an overview of the Westgate attack, discussing the tactics used and numbers of people killed and injured. He then discussed the likelihood of the identified Twitter accounts being genuinely linked to al-Shabaab. Mair proposed that the accounts were genuine due to the strong grasp of al-Shabaab history and leadership structures that the accounts displayed. He then discussed the methodology of the paper, explaining that each tweet was assessed on its content, the motivation behind it and the audience that it was designed to target.

The vast majority of tweets did not link to an external website, reference other Twitter users or utilise images. Mair argued that this was a deliberate choice taken by al-Shabaab in order to retain a large audience on Twitter by not directing individuals to other news sources and retain control of the

narrative by not engaging in debates with other Twitter users. Mair hypothesised that images were not generally used on the Twitter feed due to the likelihood of the images containing the corpses of unarmed civilians executed by the attackers. The inclusion of these images would potentially have disturbed the audience and turned them away from the Twitter feed. Additionally, their use would detract from the tone of the Twitter feed, which was presenting al-Shabaab as protectors of Somalian civilians from brutal Kenyan military oppression.

Mair's analysis showed that the majority of tweets were innocuous in nature. Only approximately 30% contained a direct or indirect threat of some description. Mair argued that this was due to the Twitter accounts' primary purpose being for publicity and propaganda as opposed to psychological warfare. Very few tweets dealt with recruitment and radicalisation, or command and control of attacks. The primary motivation of al-Shabaab's use of Twitter during the Westgate attack was to further their ideology and justify the attack.

The main audience of these tweets was identified as being the Kenyan population. The West and the media received very few directed tweets. Mair argued that this suggests that groups like al-Shabaab are geographically focused with distinctly political objectives.

Terrorist Cell Online Funding

Andrew Crocker, Founder and Chief Executive, Protect 2020 Ltd

Crocker's paper presented some of the main factors and considerations in how terrorists raise funds through their Internet activities. Crocker began by stating that funding terrorism is a relatively easy task with most attacks costing less than £10k. The September 11 attacks in 2001 however alerted government officials to the issue of terrorist funding and highlighted the need to address the issue of funding as a critical factor in disrupting terrorist activity. Security Services were thus prompted to introduce a number of checks and regulations to disrupt the movement of funds in order to prevent attacks.

Crocker pointed out that it is not the raising of funds that lends itself to disruptive tactics, but the movement of funds that opens opportunities for thwarting potential attacks. Contrary to popular belief Bin Laden did not have access to any significant amounts of personal wealth and did not personally fund al-Qaeda. Instead, £30m per year of funds was raised mainly by diversions of money from Islamic charities and the use of well-placed financial facilitators who gathered money from both witting and unwitting donors.

Since the 9/11 attacks it has been far more difficult to move money following the introduction of the USA PATRIOT Act and other punitive measures including those pertaining to money laundering. Consequently, there has been a shift away from central funding by terrorist groups to a more independent and fragmented cell system. Within this system, the ability to raise funds on the Internet relies on some critical factors: anonymity; access to criminal forums; and, the ability to transfer payments.

Anonymity is important not only for accessing the Internet for fundraising purposes but also for communicating. Crocker demonstrated that there are a number of programmes and systems available that allow users to both access and communicate anonymously for the purposes of raising and moving funds. These include the widely known TOR — an onion network that allows users to hide their identity by passing network connections through layers of TOR nodes. The Amnesic Incognito Live System (TAILS) is an operating system on a thumb drive that retains anonymity on all communications. Other methods include peer to peer chat systems that provide access to secure emails that cannot be read by interceptors.

The second critical factor for raising and moving funds is access to criminal forums. Crocker pointed out that there are a various criminal forums online that are relatively easy to find and offer ways of raising large amounts of funds. An example is criminal forums that offer stolen credit card details

that can then be cashed out via online gambling sites. While these forums are relatively easy to locate, they are not easy to join.

The final critical factor is the ability to transfer payments for the purposes of funding terrorist activity. Virtual currencies such as BITCOINS have become the preferred payment method for the purchase of stolen financial data that can then be used to fund activities. BITCOINS and other crypto-currencies can be purchased and laundered anonymously via several online services.

In closing, Crocker highlighted that the Internet provides terrorists with the tools to remain anonymous online while criminal forums and virtual currencies provide the means of fundraising to support self-funding for fragmented and decentralised cells.

Panel two

Internet Preachers and Online Propaganda: The Path to Jihad

Angela Gendron, Carleton University

Gendron began her paper by discussing the pathways that individuals take into extremism and the homegrown threat emanating from within: from young people living in Europe and North America who are inspired, radicalised and drawn into terrorism by ideologues, radical preachers and clerics who propagate al-Qaeda's revolutionary and violent interpretation of Islam either in person or by their online presence and materials. The 'homegrown threat' is of particular concern, she says, because it is analogous to a 'fifth-column' of citizens or long term residents who repudiate the values of the society in which they are embedded.

The need to understand the radicalisation phenomenon i.e. when, why and how people living in a democracy become radicalised and susceptible to militant Islamism, has been at the centre of academic and public debate for some years. Three broad research approaches have informed our knowledge so far: French sociology; social movement and social network theory; and, empiricism. They should be seen as complementary rather than competing since they focus on different levels of analysis and different aspects of the phenomena. Many identified factors reinforce rather than contradict each other but, in sum, they indicate that a range of psychological, social and environmental factors render some individuals more susceptible to militant Islamism than others.

A Dutch empirical study of jihadi activities in the Netherlands identified four typologies of terrorist actors: illegal foreigners; active and reformed criminals and addicts; 'seekers'; and, idealists and political activists. Of these, it is the idealist and political activists who are driven by social, external factors – rather than personal vulnerabilities and needs – and therefore it is they who are particularly susceptible to the perceptions of injustice they derive from television images, videos, audio tapes, websites, online sermons or the stories of others when they turn to religiously inspired ideology to explain the injustice in the world and justify a violent response to counter it.

While trusted peer relationships and kinship are important to the process of radicalisation and recruitment as indicated by social movement and network theory, evidence suggests that the Internet is the primary medium by which potential recruits to jihadism are exposed to the influence of the radical revisionist ideas which inspire Muslims around the world to engage in terrorism at home or undertake jihad as foreign fighters in conflict areas around the world.

For idealists and activists in particular, the influence of al-Qaeda's propagandists and preachers – whether in person or over the Internet – is likely to be crucial. Of the four identified typologies, they are the most likely to find answers in al-Qaeda's narrative and use them to motivate others within their social network. As a group, they travel the path to jihad together under the spiritual guidance of preachers.

Gendron further asserted that since idealists and activists tend also to be the leaders of the bottom-up or horizontal process of radicalisation which occurs within a group of radical peers, the online materials provided by jihadist preachers fuel the recruitment process both directly and indirectly: the Internet has become a virtual jihadi headquarters for self-radicalising Muslims in that it acts as a knowledge bank which they may access with ease and anonymity.

Drawing upon a Canadian study into the radicalisation of a group of young Muslims who finally left their homes to fight abroad, Gendron enumerated the ways in which the late Anwar al-Awlaki and other radical preachers use the Internet to groom young Muslims into accepting al-Qaeda's interpretation of true Islam and the necessity for violent jihad. Al-Awlaki's lecture series 'Constants on the Path of Jihad' and his guide "44 ways to Support Jihad' are together among the most frequently downloaded and circulated jihadist materials on the Internet.

Gendron drew attention to the charismatic nature of the preachers, the powerful and convincing nature of their arguments in promoting al-Qaeda's narrative, and the certainties it offers young Muslims in search of knowledge, identity and explanations. Online materials are used by cell leaders to engage their peer groups in a process of self-radicalisation while preachers use the Internet to extend their global reach and identify potential recruits by participating in interactive sites.

A prime function of propagandists, Gendron pointed out, is to present al-Qaeda's political and religious doctrine in a form which is intelligible and digestible to particular target audiences. Jihadist preachers act as mediators between the ideological pronouncements of al-Qaeda's leaders and Muslims who speak little or no Arabic and have little knowledge of Islamic thought and ideology. By providing selective English translations and interpretations of key Koranic texts and the pronouncements of al-Qaeda's ideologues, jihadist preachers can draw Muslims living in the West into the worldwide Muslim ummah and win recruits for al-Qaeda's global jihad.

To conclude the presentation, Gendron referred to the five 'constants' which al-Awlaki identified as unchanging and non-negotiable with respect to jihad and the duty of every capable individual Muslim. The Internet has enabled jihadist preachers to undermine the influence of more traditional conservative clerics in the West by exposing young Muslims to radical Salafist militancy in defence of Islam and the restoration of rule by divine law in Muslim lands. As a consequence, increasing numbers are taking the path to jihad either as foreign volunteers in various al-Qaeda fighting fronts or by carrying out attacks against the societies in which they are embedded.

Waging War on the Ideological Battleground: Terroristic Narratives and Counter Narratives Online

Dr Anne Aly, Curtin University

Aly began her paper by addressing the need for a soft power approach to effectively countering the emergence of online terroristic narratives. She argued that the success of soft power approaches relies heavily on the issue of credibility and suggested that the al-Qaeda narrative has, for the most part, been successful at attracting and influencing because of its credibility to its target audience.

Terroristic narratives online are an essential ingredient in the overall terrorist campaign. The act of terrorism itself, apart from causing massive destruction, is limited in its capacity to communicate little more than hatred and rage. For this reason, terrorists rely heavily on their ability to disseminate propaganda through online media channels — their soft power. Aly drew attention to the fact that terroristic narratives draw on master narratives that are embedded in the cultural and historic traditions familiar to their target audiences. These master narratives are easily adapted to contemporary contexts and facilitate the regenerative capacity of the terroristic narrative — its ability to be told and retold for a different time and a different context by disparate groups and individuals. The elements of the master narrative are consistent: ongoing war against Islam; corruption of Muslim rulers who cooperate with the West; Muslim injustice and the need for revenge; obligation to wage violent jihad; self-agency; and, the restoration of Islamic rule.

Aly suggested that the terrorist narrative works for two reasons: firstly, because terrorists know their audience; and, secondly because there has not been an appropriate response. According to Aly, the terrorists' audience has not been the subject of significant research. She identified six characteristics that should be taken into account for understanding the audience: transnationalism and the emergence of Muslim diaspora; shared victim identity among a growing number of Muslims worldwide; disengagement with Western media sources, by young Muslims in particular, which drives them to seek out alternative sources of news and information; access to new media platforms; perceived presence of a personal and communal crisis expressed as the survival of Islam; and, waning soft power in the Middle East and Muslim countries. Aly also identified the reasons why the counterterrorism response has not appropriately or effectively produced a counter narrative, highlighting that the 'war on terror' narrative primarily frames counterterrorism as a hard response

with a lack of focus on soft power and has not made a strong case for the non-violent action. Aly called for further research into understanding narratives with a particular focus on the audience and credibility.

Against a backdrop of waning Western influence and soft power in those parts of the world that it seeks most to influence, the issue of establishing credibility has become critical to the objective of developing a viable online counter narrative. To illustrate this, Aly presented the case of the Say No to Terror campaign. The campaign, in Arabic, consists of a full web presence including social media and a number of videos that are occasionally aired on Arabic television. Aly presented an analysis of the campaign including some examples of the website posts and the videos.

Aly drew attention to the elements of Say No to Terror that contribute to its effectiveness as disruption, concluding that the campaign lacks the essential element of credibility. In closing, Aly offered suggestions for the development of effective online counter narratives. They include knowing the audience, establishing credibility of source and message and offering viable alternatives to armed struggle.

Violent Online Radicalisation? Weighing the Role of the Internet in Past, Present, and Future Terrorism

Dr Maura Conway, Dublin City University

Conway began her paper by discussing the disconnect that exists when attempting to distinguish the 'real' world from its online counterpart and the assumptions that have been made in relation to how the Internet affects campaigns by terrorist groups. Conway explained that the Internet has made a significant contribution to terrorists' objectives, pointing out that terrorist groups can raise both finances and manpower through the Internet in addition to disseminating propaganda. She questioned the validity of commentary that dichotomises the Internet and the real world. To illustrate, she offered several examples. One of these was taken from a report produced by the Home Affairs Select Committee, which stated that the social process of radicalisation will rarely be found in online environments. Conway argued that this analysis fails to take into account the fact that the Internet is itself a social phenomenon.

Taking a step back and analysing the existing research into violent online radicalisation, Conway argued that three basic questions have yet to be answered: (1) Is it possible for an individual to be radicalised online? (2) Can online radicalisation cause individuals to become violently radicalised? And, (3) If violent radicalisation can happen, what is the process by which it occurs? So far, Conway argued, no satisfactory answers have been provided to any of these questions, with most research relying on opinion or anecdotal evidence. Conway further argued that to date research has focussed largely on the content of extremist websites and terrorist productions, not on the consumers and creators of this content. Furthermore, little to no research has focussed on the intentions of the creators of terroristic content and the role that it plays in violent online radicalisation.

To combat this gap in the literature, Conway argued that there are five steps researchers should take: (1) Look beyond jihadis, as not all terrorism is Islamist in nature; (2) Deepen and enhance the methodologies used in violent online radicalisation research. Online interviews and ethnography are valid research methodologies that could be used to study this phenomenon; (3) Scale up data collections to include large-scale data. Researchers should be using all of the tools available to them in order to analyse their data; (4) Conduct comparative analysis across various platforms. Terrorist groups operate across Facebook, Twitter and YouTube (and other platforms). Terrorism researchers should do the same in order to gain a deeper understanding of the groups they study; and, (5) Learn lessons from other Internet research. A great deal of research has been done on other online groups, such as pro-anorexia websites and suicide-support groups. Sharing best practise between researchers will provide better methodologies that assist in underpinning worthwhile research.

Conway concluded her paper by discussing how improved communication strategies have transformed terrorism and warned that future advances in the Internet would be seized upon by terrorist groups to achieve their objectives.

Panel three

Estimating the Likelihood of Cyberterrorism From a Cost-Damage Perspective

Prof Thomas Chen, City University

Chen began by contrasting the estimated costs of physical attacks and large-scale cyberattacks. Whilst a car bomb costs roughly US $15,000, and the 9/11 attacks cost roughly US $400,000, Giampiero Giacomello has estimated that a cyberattack on a hydroelectric dam would cost roughly US $1.2m and an attack on an air traffic control system would cost US $2.5m.

Chen then outlined previous work, which constructed a Malware Cost Model in order to estimate the cost of developing Stuxnet-like malware. This model consists of four parts: reconnaissance; attack code development; testing; and delivery. Using this model, the total estimated cost of Stuxnet is between US $900,000 and US $2.4m. This estimate is broadly consistent with other estimates produced by Symantec and the Langner Group. It supports the cost-damage argument, which states that the reason there have been no cyberterrorist attacks to date is the higher cost of cyberattacks relative to traditional physical attacks.

Chen then considered whether it is possible that malware costs could drop drastically in the future. He outlined four possible scenarios, rejecting the first three of these as improbable: namely, that the costs of developing new malware will drop; that Stuxnet could be reused for other targets; and, that terrorists will purchase malware from criminals at a low cost. Instead he focussed on the fourth scenario: friendly nations give terrorist groups malware for free. He pointed out that there are many historical examples of nations helping terrorists with the same political goals in order to use them as proxies.

Focussing on this possibility, Chen then outlined a model for estimating the likelihood of cyberterrorism. This employed three variables: first, the nation's level of cyber capability (i.e., their ability to create Stuxnet-like malware); second, the nation's level of support for terrorists; and, third, the cyber capability of the terrorist group. For each variable a score of zero, one, two or three is awarded. The three scores are then multiplied together to produce an overall score (maximum: 27).

Employing this model, Chen found that the greatest threat emanates from Iran. However, even the score for Iran was only nine out of 27. Overall, then, the likelihood of cyberterrorism is low. Chen concluded by noting that the reason for the low scores is that the cyber capabilities of terrorist groups are low (none scored higher than one out of three). The threat level may change therefore if terrorists' cyber capabilities improve in the future. Chen also highlighted the importance of further work aimed at producing more accurate assessments of the cyber capabilities of nations and terrorists.

Can Cyberterrorism Exist?

Clovis Meath Baker, Royal United Services Institute

Meath Baker began by discussing what we mean by cyberterrorism. Offering a practitioner's perspective, he explained that he was focussing on how the concept is used. In other words, he was offering a classification system as opposed to a dictionary-style definition. The essence of terrorism, he argued, is the threat or use of violence by non-state groups for political purposes. Terrorism must involve some threat to human life. Violence that is restricted to property only, with no risk to life, is not treated as terrorism by the political system. There must also be "blood on the walls". Acts which are designed to be merely disruptive do not qualify as terrorist.

Meath Baker then emphasised the distinction between terrorism enabled by the Internet and terrorism delivered by the Internet. The former category is extremely broad and would encompass virtually all contemporary terrorist attacks (since they almost inevitably involve online communication or planning). Therefore, only the latter should qualify as cyberterrorism.

With these qualifications in mind, Meath Baker stated that no cyberterrorist attack has occurred to date. There have been attacks on websites, but these have been merely disruptive not terrorist. For an attack to qualify as cyberterrorist it would need to be on a similar scale to Stuxnet.

Meath Baker then considered the future likelihood of cyberterrorism. He focussed on four considerations. First, capability. He emphasised that the difficulty of building cyber weapons should not be underestimated, and pointed out that cyber weapons tend to be single use (since once they have been used they can be defended against). This led on to the second consideration, intent. Although terrorist groups mount disruptive cyberattacks such as DDOS, these are not technically sophisticated and there is no indication that terrorists have the ambition to develop sophisticated destructive cyberattack tools. Cyberattacks lack the aspects of personal risk and martyrdom that make physical attacks attractive to terrorist groups. Third, vulnerability. Our cyber defences are improving as cybersecurity moves towards a behavioural approach. Fourth, impact. Whilst an attack like Stuxnet may be attractive in the context of state-on-state action (since it is deniable and there are problems of attribution), it is not such an attractive option for terrorist groups. Cyberattacks lack the impact of physical attacks. Indeed, they may often feel more like the result of industrial action or breakdown.

When these considerations are combined, cyberterrorism does not appear to be a significant risk at present. However, Meath Baker concluded by suggesting that things might change. He pointed in particular to the development of the "Internet of Things", warning that this could render individuals more vulnerable to cyberattack in the future.

Panel four

'Imagining Cyberterrorism': How US Presidents Constructed Cyberterrorism

Lella Nouri, Swansea University

Nouri's focus was the presentation of cyberterrorism within US elite political discourse. She began her presentation by contextualising her research within the field of Critical Terrorism Studies (CTS). Nouri explained that her work is in line with contemporary constructivist explorations of the discursive imaginaries at play in the invention of the terrorism threat and explores the relationships between discourse, identity and policy in the construction of cyberterrorism.

Following Ernesto Laclau and Chantal Mouffe's approach to discourse theory, Nouri explained that the purpose of her deconstruction of cyberterrorism as a national security threat in US political discourse is to chart and explain the hegemonic meanings and understandings attributed to cyberterrorism and reveal how these result from political decisions. She then moved on to explain how she collected her empirical data and justified her choice of discourse: firstly, in terms of timeframe, she selected 1993-2012 as it was during the late 1990's that the Internet and changes in technology started to affect US policy and 2012 was the end of Obama's first period in office; secondly, she chose to focus on elite presidential discourse because of its unique position of power and its influence on other sites of discourse (for example, the media).

Nouri then presented an overview of the narratives she has identified within President Bill Clinton and President George W. Bush's discourse, in terms of the initial official writing of the cyberterrorism threat. She explained that she has identified three key articulatory moments in this writing. The first is the representation of cyber threats as a product of temporal discontinuity from previous eras. Each administration write their time in office as one characterised by the advent of change and transformation and one that can be contrasted with the more considered, rational time that preceded it. The second is the related construction of the US's multifarious borders as more open than ever before and therefore that the US is more exposed to 'new' threats, including cyberterrorism. Finally, the third moment is the juxtaposition of the benefits of, and threats from, technology.

For the remainder of her presentation, Nouri provided examples of these narratives. She began with the representation of cyber threats within the narrative of temporal discontinuity as presented by Clinton's 'modern era'. She explained that the Clinton administration constructed a modern era epitomised by a resonant insecurity that is positioned as fundamentally oppositional to the Cold War era before it. Within this part of her discussion she also demonstrated Clinton's construction of a 'free and open hence vulnerable America' and the narration of technology as a force of good and bad. Nouri then turned to the construction of cyberterrorism within the Bush administration's discourse, noting similar narratives. Besides these observations she also noted how 9/11 marked a change in representations of terrorist use of the Internet and technology.

To conclude, Nouri outlined the importance of constructivist studies. She argued that by deconstructing understandings of cyberterrorism it is possible to identify alternative meanings and make space for less dominant discourses. For, this she suggested a number of think points emerging from her research. These included: what policy responses have these representations of cyberterrorism made possible? What does this construction of cyberterrorism in US political discourse do in terms of apportioning responsibility and responding to challenges? And, what actors are targeted or created in the narration of this threat?

Destruction, Uncertainty, and Vulnerability: Examining the Construction of Cyberterrorism within the Internet Security Industry

Andrew Whiting, Swansea University

In this presentation Whiting looked at how twenty different companies within the IT security industry (including the likes of Symantec, Kaspersky, and McAfee) have covered the concept of cyberterrorism and how they have constructed it within their expert discourse.

Whiting began with some introductory remarks about the rationale for his research including the opportunity to study a body of literature that thus far remains largely unexplored and has an integral role in producing knowledge around cyberterrorism. Whiting also outlined how he collected and analysed these documents, noting that he had studied over 700 documents in total.

The majority of Whiting's presentation consisted of three sections reflecting the three themes in the title. First of all was destruction. Here Whiting pointed out how cyberterrorism in this space had been constructed around the notion of destructiveness, often compared in terms of damaging potential to the September 11th attacks or other tangible examples of physical destruction such as Hurricane Katrina or Pearl Harbour. He also noted a concerted effort within this space to solidify the concept as a reality that it is no longer appropriate to think of as fictional, with an increasing effort being made to link it to empirical examples.

Next Whiting looked at uncertainty, which he broke down into three fears: of the unknown, of the future and of the unknowable. Whiting noted how the 'stealth' of cyber threats is highlighted across the industry with great emphasis put on zero-day vulnerabilities as a means of executing attacks unbeknown to the victim. The future, Whiting argued, is constructed in a manner that stresses a lack of clarity and thus requires constant vigilance. With the technology changing so rapidly there is a sense within the industry that we do not know what the cyberterrorist threat will look like tomorrow, this speculation breeding a certain anxiety surrounding the future. Finally, Whiting considered the fear of the 'unknowable' and here he focused on the complexity of the threat. The cyberterrorist threat is conveyed through extensive use of the cyber lexicon and a technical language that is difficult to comprehend and understand without prior expert knowledge.

Having established the purported destructiveness and uncertainty of the concept Whiting looked at the vulnerability associated with it. Human dependence was deemed to be a particular aspect that makes us vulnerable to the threat of cyberterrorism, as was the exponential increase in the number of different threats. The industry also stresses the 'extreme weakness' of the systems that oversee our critical infrastructure, and how the crippling potential of cyberterrorism will only increase as more and more of our society becomes computerised. Finally, Whiting looked at simplicity and the dominant belief of these companies that cyberterrorism – despite being big, sophisticated, and complex – is actually very easy to execute with the barrier of entry for cyberterrorism being very low.

In his conclusion Whiting stressed how this was the necessary first step in his research and provided an outline of where he intended to go with this work. He laid out his intention to return to this material to search out minor and dissident voices that stand in stark contrast to the dominant understanding outlined in his presentation. The purpose of this would be to highlight the contingency surrounding the concept and conduct an emancipatory project that sought to open up the concept of cyberterrorism in a manner that will hopefully allow for a reconfiguration of how we understand the concept and, in turn, how we consider related security policies and practices.

Panel five

Cyber Surveillance from a Security Perspective

Sergei Boeke, Leiden University

This presentation focussed on the debate over security concerns and privacy interests, or as Boeke characterised it, between Clapper and Greenwald. Boeke highlighted the issues of credibility surrounding the security services in light of the evasiveness with which they have responded to questions surrounding their surveillance operations. He also highlighted the imbalance of this debate and how journalists such as Glen Greenwald do not bear the same responsibility for national security that government institutions do.

Boeke contextualised surveillance practices by providing an overview of different aspects of surveillance such as CCTV, ANPR, social media, GPS, and browsing behaviour, pointing out the significant implications of this enormous growth in data. The combination of all this data and the ability to download and survey it could combine to produce an effective police state and raises alarming questions about who can be said to own this data.

Boeke stressed that surveillance should be differentiated from espionage. Espionage, in a traditional sense, focuses on military, political and economic targets of both foes and allies. Whilst there is a large body of international law and jurisprudence on when war is legal and which actions are allowed during conflict, there is no international legal framework in place that forbids espionage. However, national frameworks do exist. But these are built on hypocrisy: essentially actions which are illegal when carried out by foreign intelligence agencies at home are warranted when conducted by national agencies abroad.

Surveillance and espionage can involve many different actors and institutions. Boeke looked in depth at data collection in regards to signals intelligence (SIGINT). Acquiring data about a suspect domestically involves targeting an individual, acquiring a legal warrant and then approaching the Internet Service Provider (ISP) for the acquisition of the data (the ISP is obligated by law to deliver the requested information). In Western democracies this warrant procedure has legal checks and is focussed on one individual. Once a target is abroad, however, this becomes a lot more difficult as dealing with ISPs and telephone providers is not possible. The net result of this is a tendency on the part of several nations to carry out 'bulk collection of information' and then conduct targeted searches in the bulk data.

Boeke highlighted the important distinction between metadata and content. Metadata does not require a warrant in many countries but still allows for a very significant picture to be built up around an individual. In the US, the collection of metadata under the Verizon program is not connected to the actual credentials (subscriber details) of the subjects, these remaining anonymous.

The next part of the presentation featured a case study of former al-Qaeda leader Osama bin Laden and the role different kinds of intelligence played in his killing. Boeke pointed to a mixture of SIGINT, HUMINT (human intelligence), IMINT (imagery intelligence, namely satellites and drones) and OSINT (open source intelligence) to track bin Laden to his compound.

Boeke asked how we can measure the effectiveness of these intelligence collecting capabilities and stated that there is a lack of research surrounding them. He questioned whether the number of foiled attacks provides a useful metric. Academic research has refuted the initial claims by the American government that the specific mass collection programs disclosed by Snowden had prevented 50 terrorist attacks, but in some cases they did contribute to counterterrorism investigations. Above all, governments are understandably wary of dismissing counterterrorism options on the premise that they were ineffective in the past. Despite a series of arguments being made about counterterrorism's effectiveness including logical arguments, themes of deterrence, dissuasion, and disruption, as well

as utilising inferences from the past there still exists the practical problem of showcasing the success of surveillance in terms of prosecutions.

To conclude, Boeke raised a series of dilemmas including the problematic distinction between national and foreign targets and the bulk interception of intelligence abroad. Now we know what the 'Five Eyes' are doing, what about other countries and private entities? Much of the discussion of late has focussed on public entities while questions surrounding the collection, storage and trade in personal data by the private sector remain comparably unexplored.

Illegal Cyber Operations and the Concept of 'Positive Obligations' of States

Dr Karine Bannelier-Christakis, University of Grenoble-Alps

Bannelier-Christakis began by pointing out that hostile cyber operations are seen as one of the biggest threats to national security. Given this, it is important to consider the legal responsibilities states have in responding to this threat vis-à-vis other states. Bannelier-Christakis explained that the concept of due diligence is significant in this regard, since it places an obligation on states to notify other states and react to illegal cyber operations. The concept of due diligence is linked to the concept of the sovereignty of states: no state is allowed to knowingly allow their territory to be used to harm another. However, there remains a problem that is difficult if not impossible to overcome: how does one prove that there was knowledge of the attacks from the transit states? And, following on from this, how could these transit states therefore be held accountable?

Bannelier-Christakis went on to provide a number of examples that highlight this difficulty. She posed the question, what is the standard of proof required to show that a transit state knew that an operation was taking place? Additionally, does our principle of due diligence apply to those who try and evade requests of due diligence because they are ignorant and should the principle extend to those who ought to know?

The presentation then moved on to consider some of the potential implications of these questions, including – notably – whether cyber operations and due diligence combine to create a requirement that states should monitor all cyber activity (something that is described as a 'cornerstone' in the recently published French White Paper of Defence). If this is indeed the case, could due diligence become a Trojan horse for the erosion of civil liberties?

Bannelier-Christakis argued that states should only be permitted to operate within the limits stipulated by international law and that cyber diligence should only allow monitoring in a manner that links with other existing legal frameworks (including human rights frameworks).

What then are the positive obligations that states need to take? Bannelier-Christakis argued that we must first recognise that positive obligations should not create an unreasonable situation for the state; an element of reasonableness should figure in our expectations. Having said this, Bannelier-Christakis argued that some legislative measures are surely required to respond to these challenges and recognise states' obligations to prevent and protect. This is something that the international strategy for cyberspace recognises as important in relation to protecting both public and private information infrastructure. But states should also be obliged to react and warn potential victims of cyberattacks and to try and terminate the illegal activity and punish the event.

Bannelier-Christakis concluded by reiterating that the concept of due diligence requires more than just a duty to terminate an attack. She argued that seeking an international agreement on cyberterrorism would be an effective way in which to make the concept of due diligence more compelling.

The Tension between Surveillance, Privacy and Rule of Law in the Digital Domain

Dr Inger Marie Sunde, Norwegian Police University College

Sunde began by explaining that she had worked previously as a practitioner and had moved into academia, helping to train the Norwegian police on the use of technology and criminal law. Her presentation highlighted the difficulty the criminal law faces in keeping pace with technology, a difficulty that can be compounded by the manner in which different law enforcement institutions each deal with the terrorist threat separately (as is the case in Norway).

Sunde then moved on to concentrate on the Anders Behring Breivik case study. Breivik may be an example of a lone wolf in execution, but not in planning. For example, he downloaded 600 bomb manuals and acquired knowledge on over 100 explosives. Sunde noted the huge backlash against Norwegian police in the aftermath of the attack and outlined how major deficiencies in police information and communications technology became evident. Recurring criticisms of the police in Norway focused on the perceived underestimation of the terrorist threat and the limited focus, concentrating on oil platforms as a target and limiting the actors to Islamic extremism and jihadism.

Post-Breivik the Norwegian police has received a lot more money, has made a lot of high tech acquisitions, and has established a cybersecurity research centre to deal with some of the weaknesses in the system. The upshot of this is a far greater expectation being placed on the police in terms of their performance.

In the light of this increased expectation, Sunde then asked how governments and police can be held accountable. Here Sunde introduced the work of Karl Olivecrona (a Scandinavian legal realist). Olivecrona's work draws a distinction between correctness (an action is either in accordance with a rule or it is not) and truth (which depends on a body/system of rules plus shared values). In the present context, these values include transparency and accountability. The ability to exercise control over surveillance practices and to hold governments accountable depends on the quality and reliability of the logfiles and reports which are generated by surveillance systems. However, this documentation will be no better than the design of the technology itself. And legislators tend to abdicate technological issues when preparing and introducing surveillance rules/powers, outsourcing them to private contractors. This results in a gap between the design of law and technological implementation. To close this gap, technological implementation should be designed according to legal requirements: law as technical fact.

Sunde concluded by outlining the direction of her future research. It will consist of three strands. The first is normative, and will consider the rule of law requirements pertaining to control and accountability. Second, an extensive document analysis will look at preparatory works on surveillance legislation and analyse how technological aspects and control issues have been addressed. And finally, a study of existing technical control functions, which will include examination of the quality and reliability of reports.

Panel six

Dataveillance and Terrorism: Swamps, Haystacks and the Eye of Providence

Dr Stuart Macdonald, Swansea University

Macdonald began his presentation with a news story from 2012 from the New York Times, concerning the US superstore Target. The story reported that data analysts had developed a pregnancy prediction model, which used data on women's purchases in order to identify those who were pregnant. The rationale was that women's shopping habits change during pregnancy, and that "if we get them buying diapers from us, they're going to start buying everything else too". Women who were identified as being pregnant were sent coupons timed to the specific stage of their pregnancy. The model turned out to be fairly accurate. In fact, the story told of one high school student who had been sent coupons before her parents had even learned of her pregnancy.

The first half of Macdonald's presentation examined whether this degree of predictive potential could be achieved in the realm of counterterrorism. He focused specifically on pattern-based queries: searches which look for patterns of activity that are indicative of a terrorist plot. The hypothesis here is that terrorist plots involve transactions that will manifest themselves in information databases. The principal claimed benefit of pattern-based queries is that they have the potential to identify individuals who have not yet aroused any suspicion - "clean skins" - meaning that terrorist plots could be identified at an early stage and attacks prevented.

Macdonald outlined four difficulties with pattern-based queries in this context. First, modelling. In the commercial context companies have enormous datasets to work from. By contrast, successful terrorist attacks are relatively rare, so the evidential basis for constructing patterns is small. Plus, working on the basis of past attacks is reactive and so may miss novel forms of attack. Second, false positives (individuals who are wrongly deemed to be worthy of suspicion). In a population of 250 million, an accuracy rate of 99.9% would result in a quarter of a million false positives. And few believe that an accuracy rate of 99.9% is achievable. As well as modelling difficulties, there is the problem of poor quality data - which is exacerbated by crimes like identity theft. Third, false negatives (individuals who are wrongly deemed to be not worthy of suspicion). Given that many terrorists use anonymisation and encryption technologies, this is a significant problem. Fourth, the combination of false positives and false negatives could result in collateral security losses. Resources and time may be spent investigating false positives while false negatives may escape attention.

Since they involve suspicion-less searches, pattern-based queries also raise important privacy-based concerns. Macdonald outlined three concerns in particular. First, techniques like data-mining make it possible to take lots of discrete pieces of data about an individual and reassemble them. Even if each individual piece of data is innocuous and not something the person would be concerned to hide, the reconstructed assemblage might be something the person would regard as private. Moreover, this aggregation might be done without the individual's permission and possibly even the individual's knowledge, which raises issues of "technological due process". Second, marketing campaigns use information databases to sort customers into categories. When this is applied in the context of counterterrorism, the power of sorting can become the power of discrimination. Sorting individuals on the basis of what is perceived as suspicious and illegitimate can impact disproportionately on particular minority groups. Third, surveillance can deter people from engaging in thoughts and deeds that others consider deviant, undermining society's commitment to intellectual diversity and individuality.

Macdonald finished by examining constitutional protection of privacy under Article 8 ECHR and the US Fourth Amendment, focussing specifically on dataveillance programmes. He explained that such programmes fall within the scope of Article 8, and so in order to be justifiable must be deemed strictly necessary in the interests of national security. This test of necessity offers courts in Europe the opportunity to scrutinise the claimed security benefits offered by a dataveillance programme and

to consider other possible investigative techniques that might be less intrusive. In the US, by contrast, it is unclear whether dataveillance programmes fall within the scope of the Fourth Amendment. Much of the information involved in these programmes would not, on their own, fall within the Fourth Amendment as a result of the public observation and third party doctrines. However, the process of aggregation should arguably be regarded as constitutionally significant - an argument that finds some support in the US Supreme Court case US v Jones. If the Fourth Amendment were held to apply, the courts would have the opportunity to exercise similar scrutiny to that found in Europe.

An Assessment Model for Improving National Cyber Security Postures

Ünal Tatar, National Cyber Security Institute of Turkey

Tatar presented his ongoing research which aims to create an assessment model for the purpose of improving national cybersecurity postures. He began by outlining three main targets of cyber threats: nations, organisations and individuals. On the basis of these threats, Tatar argued that we need to develop different levels of countermeasures: macro, for those targeted at nations and as such effect critical infrastructure; meso, for those threats that are targeted at organisations and/or group system users; and, finally, micro, for those attacks targeted against individuals such as phishing mails.

Tatar explained that his assessment model focuses on macro threats, i.e., those involving national cybersecurity. He began by providing an overview of the major challenges to countermeasures in this area. These include: the complexity of managing the cybersecurity of critical infrastructure; the difficulties that exist in coping with targeted attacks (e.g. attribution problems); lack of capacity (e.g. not enough workforce in cybersecurity); and, obstacles in information sharing (due to the constraints of data protection across national lines). Tatar contextualised these problems by showing how the number of national cybersecurity strategies has dramatically increased since 2007 (the Estonia case) and again since 2010 (with the news of Stuxnet).

In the remainder of his presentation Tatar explained his working assessment model using the case study of the Turkish National Security Strategy. The premise of the model is that a stage by stage process for risk management is necessary. Tatar's model involves four stages. The first is a threshold stage, and involves defining what constitutes a macro cybersecurity threat. The second considers what actions are needed in response to the threat. The third asks who will take that action. The final stage then involves an assessment of the current situation. Tatar argued that this model simplifies the decision making process for reorganisation and reauthorisation with a risk management perspective.

The threshold stage of the proposed framework involves a number of parameters, which have to be defined not only on a case by case basis but also by each nation to fits its own needs. For Tatar, relevant considerations include: whether there is an imminent threat of fatalities; possible economic consequences; the likely impact on the country's national security capabilities; the identity and number of organisations targeted; the identity of the perpetrator; the likely impact on specific sectors; and, the political setting.

To conclude, Tatar used his model to construct a roles and responsibilities matrix. The matrix distinguished three parts of risk management (asset, vulnerability and threat) at three different stages (before, during and after a cyber incident), and applied this framework to both detection and response. For each specific scenario Tatar identified potential countermeasures.

Who's on First? The Public Private Partnership in National Cybersecurity Strategies

Dr Madeline M Carr, Aberystwyth University

Carr's presentation examined the public – private partnership, often referred to as P3, in national cybersecurity strategies. She began by explaining that P3 is the cornerstone of many national cybersecurity strategies. However, the relationship is inherently problematic in this context, for two main reasons. First, P3 disrupts the established expectation that it is the responsibility of the state to safeguard national security. And, second, despite its centrality, P3 arrangements for cybersecurity are indistinct, with unclear lines of responsibility. Carr explained that acknowledging these challenges is essential for the development of a sound strategy.

Carr then moved on to discuss P3 and its problems in greater detail. She began by summarising the promises surrounding the long history of public – private partnerships. Carr explained that the reason these partnerships form is that neither party can reach their goal alone. These partnerships are normally underpinned by clearly drawn lines of responsibility and authority, as well as mutual obligations and trust. Carr then discussed how governments and the private sector view P3 in the specific context of national cybersecurity. Governments, she argued, see the P3 relationship as: a joint and shared pursuit; a solution to the mandate and capability gap; an area that the private sector should and can take the lead on; and, a space for information sharing between the two sectors. In stark contrast, the private sector: do not expect to fund national security; are unwilling to accept liability for the provision of national cybersecurity; and, are reluctant to share their own information (though they expect timely and actionable information sharing from the government).

Carr then examined the implications of this difference in expectations. She explained that P3 is dependent upon shared goals and clear lines of responsibility, both of which are lacking in this context. She also noted that profitability is often incompatible with the provision of a 'public good' and therefore questioned whether it is feasible to outsource national security and whether the private sector ever would – or should – accept liability.

Carr concluded by sharing a number of think points. These included: if critical information infrastructure is now regarded as integral to national security, and we rely on P3, how well equipped is the state to carry out this core function? And what are the implications for national and international security?

Conclusions and Recommendations

A wide range of topics were addressed in the course of the symposium, including the possibility of cyberattack, a broad range 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 (for example, of the question whether cyberterrorism has ever occurred), but also have important practical ramifications (for example, in developing models of risk management). It is also important to recognise that some of the different understandings of cyberterrorism are the product of particular interests or concerns. Deconstructing these understandings opens up a range of other important research questions and also creates space for dissident voices.

Transnational: Many online terrorist activities now transcend national boundaries. Terrorist publicity, propaganda and radicalisation campaigns all now have a global reach. Terrorist financing is also increasingly transnational in nature. As a result, counterterrorism also needs to be transnational. International law has a significant role to play, and international cooperation is essential. At the same time, however, 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: The vulnerability of different actors was a recurring theme. First, nation states, and in particular their critical infrastructures, are frequently portrayed as susceptible to attack. Cyberspace itself is also often presented as inherently vulnerable, with techniques like anonymisation and encryption and problems of attribution presented as giving terrorist groups a key strategic advantage. Second, citizens are often presented as being vulnerable too – in some cases to the threat of radicalisation, and in others to cyberattack or other forms of cybercrime.

Credibility: Credibility was also a key theme. First, the credibility of terroristic narratives and counter narratives is important. Interestingly, the qualities that confer credibility may be different for terroristic narratives and counter narratives. Second, there are issues surrounding the credibility of governments' counterterrorism laws and policies, and the discourse surrounding these. This is particularly apparent in the case of cyber surveillance.

Power: It was evident from the range of papers presented that terrorist groups employ both hard and soft power in pursuit of their objectives. Whilst counterterrorism frequently employs hard forms of response, questions were raised concerning the extent to which governments employ soft forms of response – and the effectiveness of soft countermeasures when they are employed.

Evidence: Numerous areas were identified where understanding is currently lacking and further research is required. These included: gaining a better understanding of the terrorists themselves, the materials they place online and their cyber capabilities; gaining a better understanding of the consumers of extremist online content; developing a more dynamic understanding of the relationship between the Internet and the offline world; analysing the effectiveness of counterterrorism laws and policies, including accountability mechanisms, and how to assess effectiveness; gaining a deeper understanding of how counterterrorism policies are produced and of how cooperation can be engendered between the private and public sectors and within the international community.

Appendix: List of Delegates

Anne Aly, Curtin University
Clovis Meath Baker, Royal United Services Institute
Arron Banfield, Swansea University
Karine Bannelier-Christakis, University of Grenoble-Alps
Burke Ugur Basaranel, Swansea University
Tina Billington-Hughes, University of East London
Patrick Bishop, Swansea University
Serge Boeke, Leiden University
Andrea Buck, Swansea University
Verity Cannell, Swansea University
Madeline Carr, Aberystwyth University
Julia Carroll, Swansea University
Tom Chen, City University
Maura Conway, Dublin City University
Andrew Crocker, Protect 2020 Ltd
Curon Wyn Davies, Swansea University
Kirstie Dunseath, Swansea University
Louise Edgington, Swansea University
Angela Gendron, Carleton University
Pete Hanratty, Swansea University
Sophia Hinde, Home Office
Savyasaachi Jain, Swansea University
Charlotte Knowles, Shoots & Leaves Films
Simon Lavis, Swansea University
Tim Legrand, Australian National University
Nuria Lorenzo-Dus, Swansea University
Colin Macdonald, Organised Crime & Counter Terrorism Police Unit Scotland
Stuart Macdonald, Swansea University
David Mair, Swansea University
Lella Nouri, Swansea University
George Oikonomou, Bristol University
Paul Peters, South Wales Police
Gary Philips, South Wales Police
Helen Quane, Swansea University
Nathan Roger, Swansea University
Martin Rudner, Carleton University
Monika Seisenberger, Swansea University
Anton Setzer, Swansea University
Inge Marie Sunde, Norwegian Police University College
Guy Szablewski, Swansea University
Unal Tatar, National Cyber Security Institute of Turkey
Katy Vaughan, Swansea University
Andrew Whiting, Swansea University

the cyberterrorism project

Contact Details

ctproject@swansea.ac.uk

www.cyberterrorism-project.org

www.facebook.com/CyberterrorismProject

@CTP_Swansea

Project Directors

Professor Thomas Chen

School of Engineering and Mathematical Sciences
City University London

tom.chen.1@city.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), *Mathematical Foundations for Signal Processing, Communications, and Networking* (2011), *Cyberterrorism: Understanding, Assessment and Response* (2014) and *Terrorism Online: Politics, Law and Technology* (forthcoming), 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

School of Political, Social and International Studies
University of East Anglia

l.jarvis@uea.ac.uk
@LeeJarvisPols

Dr Lee Jarvis is Senior Lecturer in International Security at the University of East Anglia (UK). His books include *Times of Terror: Discourse, Temporality and the War on Terror* (Palgrave, 2009); *Terrorism: A Critical Introduction* (Palgrave, 2011, with Richard Jackson, Jeroen Gunning and Marie Breen Smyth); *Cyberterrorism: Understanding, Assessment and Response* (Springer, 2014, co-edited with Tom Chen and Stuart Macdonald); and, *Counter-Radicalisation: Critical Perspectives* (Routledge, 2014, co-edited with Christopher Baker-Beall and Charlotte Heath-Kelly). His research on the politics of terrorism, counterterrorism and security has been published in journals including *Security Dialogue*, *Political Studies*, *Millennium: Journal of International Studies*, *International Relations*, *Terrorism and Political Violence* and *Critical Studies on Terrorism*.

Dr Stuart Macdonald

College of Law
Swansea University

s.macdonald@swansea.ac.uk
@CTProject_SM

Dr Stuart Macdonald is Associate Professor in Law at Swansea University (UK). He has written a number of articles on counterterrorism legislation and policy which have been published in leading international journals, including *Terrorism and Political Violence*, *Studies in Conflict & Terrorism*, *Sydney Law Review*, *Criminal Law & Philosophy* and *Cornell Journal of Law and Public Policy*. He is co-editor (with Lee Jarvis and Tom Chen) of *Cyberterrorism: Understanding, Assessment and Response* (Springer, 2014) and *Terrorism Online: Politics, Law and Technology* (Routledge, forthcoming). He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney. His project on security and liberty was funded by the British Academy.