Advanced Research Workshop supported by the NATO Science for Peace and Security Programme

Terrorists' Use of the Internet: Assessment and Response

Final Report

September 2016

NATO OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme

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), constructing a database of international definitions of cyberterrorism and conducting a study of media constructions of cyberterrorism. Findings from these activities have been published in top international journals including *Terrorism and Political Violence*, *Studies in Conflict and Terrorism*, *Perspectives on Terrorism*, and, *Journal of Terrorism Research*, and in books including *Cyberterrorism: Understanding, Assessment and Response* (Springer, 2014), *Terrorism Online: Politics, Law and Technology* (Routledge, 2015), and, *Violent Extremism Online: New Perspectives on Terrorism and the Internet* (Routledge, 2016). 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. 43).

Preface

This report contains findings from the Advanced Research Workshop supported by the NATO Science for Peace and Security Programme on terrorists' use of the Internet, held at Dublin City University on 27th-29th June 2016. The event was co-organised by the Cyberterrorism Project and the VOX-POL Network of Excellence. The workshop consisted of a total of 31 presentations, followed by a roundtable discussion during which participants formulated a set of recommendations. 60 delegates attended the symposium, from 13 different countries, including researchers and representatives from NATO HQ, NATO CCD-COE, UNICRI, the European Defence Agency, the Bavarian Police Academy and the Italian Carabinieri.

This report provides summaries of each of the presentations and presents the workshop's final recommendations

Organisation Committee

The members of the workshop organization committee were Prof Stuart Macdonald (NATO country Co-Director), Prof Maura Conway (NATO partner country Co-Director), Dr Lee Jarvis and Unal Tatar.

Acknowledgements

We would like to thank NATO's Emerging Security Challenges Division, the VOX-POL Network of Excellence, Dublin City University and Swansea University for supporting the workshop. We would also like to thank Joseph Dillon, James Fitzgerald, Bethany Gaines, Sarah Holtom, Loni Lee, Orla Lehane, Sean Looney, Lisa McInerney, Lella Nouri-Bennett, Katerina Pitsoli, Lucy Ray, Adam Ridley, Ryan Scrivens and Andrew Whiting for assisting with the hosting of the event, and Simon Lavis for his work on the production of this report.

Suggested Citation

Conway, M., Macdonald, S., & Mair, D. (2016). *Advanced Research Workshop supported by the NATO Science for Peace and Security Programme, Terrorists' Use of the Internet: Assessment and Response – Final Report*. Cyberterrorism Project Research Report (No. 6). Available via: www.cyberterrorism-project.org

Table of Contents

Introduction

Two of the global threats identified by the US Intelligence Community's 2016 Worldwide Threat Assessment were cyber and technology, and terrorism. The aim of this workshop was to examine the convergence of these threats.

It is well-known that terrorist organisations already make wide use of the Internet. Online terrorist activities include:

- Radicalisation and recruitment: Recruitment and radicalisation are amongst the top priorities for terrorist organisations online. This is unsurprising, since the worldwide reach of the Internet provides terrorist organisations with a global pool of potential recruits.
- Propaganda: Terrorist organisations use a range of social media and multimedia formats. This gives them direct control over the distribution and reach of their message and of its content, allowing them the opportunity to shape how they and their adversaries are perceived by different target audiences.
- Planning: Much of the information needed to plan a physical attack is publicly available online, numerous tools are available to facilitate data collection and online searching capabilities allow terrorists to capture information anonymously and with little effort or expense, while mitigating the risk involved in offline reconnaissance operations.
- Communication within terrorist groups: Email allows for asynchronous communication, whilst Internet Relay Chat applications such as Skype can be used for synchronous communication in conjunction with anonymising software.
- Training: The range of resources that are available online, from bomb-making manuals to instructional guides on encryption and surveillance avoidance, mean that the Internet has the potential to operate as a virtual training camp.
- Fund-raising: Terrorist organisations have used various methods to raise and transfer funds online, including: direct solicitation; selling CDs, DVDs, badges, flags and books; diverting funds intended for seemingly legitimate organisations like charities; and, cybercrime such as identity theft.
- Cyberattack: Terrorist organisations have expressed an interest in developing offensive cyber capabilities. These include the strategic use of malware as a weapon.

The aims of the workshop were therefore as follows:

- To assess the threat of terrorists launching cyberattacks and evaluate methods of improving protection of critical infrastructure;
- To deepen existing understanding of the different ways in which terrorists use the Internet and produce recommendations for the formulation of laws and policies to counter this threat;
- To evaluate these legislative and policy responses in terms of their impact on democracy, liberty and the rule of law;
- To generate innovative, interdisciplinary and robust methodologies and techniques for the study of terrorists' online activities; and,
- To evaluate 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.

A further aim of the workshop was to nurture dialogue between members of the academic, policy and practitioner communities. The participants therefore included representatives from each of these communities. As well as bridging the gap between academia and practice, the workshop also sought to bridge disciplinary divides. The participants had a wide range of expertise (including engineering, computer science, law, criminology, political science, international relations, history, and linguistics).

This report provides summaries of each of the presentations and presents the workshop's final recommendations.

Cyberterrorism: Assessment and Response

Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications

Dr Hayrettin Bahşi, Tallinn University of Technology

Bahsi addressed the impact of 'Internet of Things' (IoT) applications on the landscape of cybersecurity, contextualising it by contrasting it to existing Supervisory Control and Data Acquisitions (SCADA) systems. He explained that the latter are often used in critical infrastructure systems (such as gas, electrics, and transportation) and thus have already undergone thorough analysis with regard to the cost-benefit equation and the potential physical result of a cyberattack.

Bahsi began by introducing the current cybersecurity landscape, which is very information centric, an approach which seeks to analyse the physical results of an attack on a critical infrastructure. He then explored the motivation of threat actors in the current landscape, illustrating that the actors' approach is a very rational one based on cost considerations and picking methods requiring the least effort and equipment in order to evade detection. Bahsi identified cyber espionage as being particularly attractive, especially among state-sponsored actors, as hacking offers a relatively safe and easy way of gaining political and economic advantage.

Bahsi then discussed how IoT applications might change the cybersecurity landscape. To this end, Bahsi considered the questions of how physical results might be created via cyber attacks on IoT applications and whether IoT applications can change the cost-benefit equation. Bahsi took a hypothetical look at smart healthcare systems as the IoT in question in order to elucidate how the landscape might change.

With regard to healthcare, Bahsi noted that systems are dominated by a concern for patient privacy, as opposed to concern for safety, which dominates SCADA systems. This difference in priorities, coupled with the lack of sophistication in connectivity technology within smart health systems, makes the health sector the most breached sub-sector. Bahsi pointed out that the emphasis on safety in critical infrastructure organisations gives an additional advantage to them in developing better contingency plans and maintenance procedures, which in turn helps to improve their incident response capabilities. Bahsi added that the collection of data over the Internet makes smart healthcare systems more vulnerable to Internet-based attacks.

In comparing the factors motivating a potential cyber attacker (e.g. physical result, probability of success), Bahsi asserted that an attack on a critical infrastructure using SCADA is less likely but probably more impactful whereas an attack on an IoT application is more likely but probably less impactful. Bahsi then concluded that the overall impact of cyberterrorist activity on IoT applications may not be as high as the impact on critical infrastructures, however they may still be a reasonable target for terrorists due to the possible physical results.

Bahsi therefore recommended that, as happened with SCADA systems, a detailed analysis of IoT applications should take place, particularly with regard to the cost-benefit equation and of the physical results of a cyber attack.

Novel Approaches for Cyber Risk Management

Dr Theo Tryfonas, University of Bristol

Tryfonas's presentation concerned the need for a strategy for cyber risk management to be both cost-effective and cost-efficient. Tryfonas assessed the current strategy for cyber risk management and suggested a novel approach to both cover the shortcomings of the traditional approach and to fulfill the need for the strategy to be cost effective.

With regard to the existing approach, Tryfonas focused on the need to protect critical infrastructures using Industrial Control Systems (ICS), which could be particularly attractive targets for cyberterrorists (e.g. a city's traffic lights control system). The current approach was described by Tryfonas as being one of risk management whereby the risk is assessed by considering the characteristics of the systems and the impact of a successful attack, after which a recommendation is made for a defence mechanism to minimise the risks.

The deficiency in this approach, Tryfonas argued, is that it is an adaptation of existing methods used to assess risks in commercial enterprise systems, and is thus tailored to that landscape, rather than to the landscape of critical infrastructures. Furthermore, there is a tendency for this approach to disregard the growing interdependence between the components within an ICS and also across different ICSs. Tryfonas was also sceptical that the existing approach has the necessary flexibility to keep pace with the evolving threat landscape and the variety and multiplicity of attacks.

The novel approach that Tryfonas suggested to address these shortcomings is an amalgamation of the Viable Systems Model (VSM) and Game Theory. To illustrate it Tryfonas explained the workings of each. The VSM that Tryfonas employed was developed by Stafford Beer in 1972, with the purpose of representing a system of interest (e.g. an organisation) through a living analogy that can be used to assess the criticality of a subsystem/asset via its interconnections to other subsystems/assets. The suggested approach does so by using a formula containing a number of variables (with values ascribed to each variable), namely the market price, the number of connections, the effect on other ICSs, and the role of the cyber component. Tryfonas then explained how Game Theory can be used to create a hypothetical game between an attacker and a defender to determine the most cost-effective strategies for both via a cost-benefit analysis.

Tryfonas concluded with an assessment of the novel joint VSM-Game Theory strategy, which he argued provides a cost-efficient defence approach that accounts for interconnectivity within and across ICSs. Tryfonas accepted, however, that the strategy requires validation against real data in order to be considered an applicable approach to protecting ICSs.

Cyber Defence in a Multinational Environment

Paul Shorte, Aide de Camp to the United Nations Head of Mission and Force Commander in Lebanon

Shorte's presentation addressed the issues of cyber defence on the various networks across NATO, considering the problems of information sharing and system degradation. Shorte first outlined the levels of policy that each network has – strategic (largely consisting of national policy), operational, and tactical – and then considered the issues of interoperability when networks must work together.

With regard to interoperability issues, Shorte highlighted the Afghanistan mission, whereby 48 troop-contributing countries had to work on a multitude of networks based on the security clearance afforded to each individual nation, i.e. "FYVE" (Five Eyes), in order to work together. Shorte explained that the reluctance of nations to grant access to their deployed systems, due to fear of disclosing weaknesses in cybersecurity, means that multinational policy will lag behind national policy. Shorte noted the challenges within the UN system and the lack of a specific cyber defence policy despite having developed policy in many other areas and cyber defence being such a significant multinational issue. Moreover, within the UN key information is often transmitted between various missions using a tried and trusted method: via fax.

Shorte then addressed the issue of information sharing, which he framed with reference to the famous Sun Tzu quote from *The Art of War* "If you know your enemy and you know yourself, you need not fear the result of a hundred battles." Focusing on the problems of NATO "knowing itself", one such problem is the huge system degradation. Shorte pointed out that many NATO systems are slowly becoming outdated, having been built for specific operating systems and outdated versions of software where known vulnerabilities exist. Shorte explained that this is of huge cost to NATO and seriously constrains its operational capability at cyber level due to it not "knowing itself".

Cyberterrorism – a challenge both for external and internal security: Countering cyberterrorism – a task for law enforcement agencies and the military in crisis management operations

Wolfgang Röhrig, European Defence Agency

Röhrig's paper began by outlining the changes in terrorism over the last 45 years, from the IRA and centralized coordination structures, to today's IS/Daesh and global missionary propagation of Islamist Ideology and the worldwide caliphate. This includes the link to cyberterrorism, where terrorists have become adaptive to 'Technology Development' in order to radicalise, recruit, fund-raise and communicate anonymously.

The increased sophistication of terrorist's use of the internet and the threat this poses needs to be handled by Crisis Management Operations. Röhrig discussed the 'Petersberg Tasks' as expanded in 2009 in the TEU article 42 as an example of crisis management operations. Röhrig then revealed that the current situation of the military is that it is becoming increasingly dependent on civilian (critical) infrastructures and services (at home and in the AoR (Area of Responsibility)) and that the military is constantly growing and becoming increasingly complex with interconnected networks (Network Enabled Capabilities (NEC)). This rapid development is due to the velocity of new threats and vulnerabilities the military faces every day.

Röhrig went on to discuss domestic substantive criminal and procedural law and the criminalisation of conduct in cyberspace. Despite this, Röhrig highlighted that within national boundaries, countering cyberterrorism is in general a task for law enforcement agencies and national regulations and policies define the role and the limitations for the engagement of the military. He then continued by explaining the military's role in counterterrorism post-9/11 involves a paradigm shift from symmetric warfare to counter asymmetric threats with military means. Due to the events of 9/11 military capabilities had to be improved by, for example, countering Improvised Explosive Devices and Longhaul communications. In order to respond to technological developments, remotely piloted systems and robotics/ autonomous systems have been created in order to access the full spectrum of electronic and digital connectivity and dominance.

Commander's/ Mission Head's key questions related to cyber along the Operational Planning Process (OPP) were then demonstrated and discussed briefly by Röhrig, by interpreting the Law of Armed Conflict (LoAC) and International Humanitarian Law (IHL) in combination with the Tallinn Manual, leading onto the complementary use of law enforcement agencies and the military in countering cyberterrorism operations. He explained that, when applying the LoAC and IHL in combination with the Tallinn Manual, cyberterrorism is not just using electronic means (cyberspace) for coordinating and sharing information of terrorist activities but the use of force that constitutes the level of an armed attack in order to spread terror. A cyberattack on military installations by terrorists does not automatically fulfil this definition of cyberterrorism.

How to Protect Critical Information Infrastructures: Roles and Responsibilities for Military, Public and Private Sectors

Dr Gokhan Ikitemur, Turkish Ministry of Internal Affairs; **Unal Tatar**, Old Dominion University

Ikitemur and Tatar began their presentation by looking into national cybersecurity from a managerial perspective, including their case study of Turkey, to demonstrate the new era, in which the lines between public and private spheres have blurred. They explained that cybersecurity is not only a technical but also a governance problem since it does not fit conventional security categories. The other underlying reasons for the governance problem are that the private sector is no longer the sole consumer of nation states' security blanket, and national cybersecurity is not a single subject area, it is generally divided into five distinct mandates (military, counter, intelligence, critical infrastructure and protection).

Ikitemur and Tatar chose Turkey as their case study because of the country's socio-economic dynamics, but mainly because Turkey is interested in developing national cybersecurity governance and therefore protecting itself against exponential cyber threats. Due to this, Turkey established a Cyber Security Council in 2012, prepared a national cybersecurity strategy for 2013-2015 and later moved onto their second strategy (2016-2019) to resolve the deficiencies of the previous one. Ikitemur and Tatar discussed different regulation mechanisms and approaches to securing critical infrastructures, which are owned or operated mostly by the private sector. The balance between regulation and cooperation (or voluntary approach) depends on several factors specific to the nation such as current governance structures, percentage of private sector ownership of national critical infrastructures, culture and level of trust between government and the private sector. According to a Delphi survey conducted on critical infrastructure operators, government regulation is almost mandatory to raise the maturity of level and cybersecurity readiness of private sector.

To conclude their paper, Ikitemur and Tatar highlighted their key findings and recommendations. They suggested that closing the gap between maker understanding and frontline realities is essential in producing a reliable cybersecurity system and that a traditional hierarchy within governance yields collaborative engagement (as new skill sets are required). 'Red Teaming' is also recommended to examine the nature of the distribution of roles and responsibilities to see if the current situation/dynamic is problematic or not. However, Ikitemur and Tatar ended their presentation by suggesting that innovative solutions are required which enhance cybersecurity without creating barriers to innovation, economic growth, and the free flow of information in order to cope with the challenges of national cybersecurity governance.

International cooperation in facing the cyberterrorism threat

Dr Camino Kavanagh, King's College London; **Dr Madeline Carr**, Cardiff University; **Adam Hadley**, ICT4Peace

This presentation examined terrorist use of the internet, ICT and cyberspace, and identified a number of emerging principles, norms and cooperative measures underpinning the response by public and private actors.

Hadley first described the manner in which the internet and ICT are being used for terrorist purposes including strategic communications, command and control, grooming, recruitment, and financing.

Kavanagh then discussed the nature of the response, including the ever-blurring line between the public and the private sphere when dealing with terrorist-related online content. Emphasis was placed on the increasing reliance of governments on technology and social media companies to remove terrorist related content and related questions of legitimacy, transparency and accountability.

With the policy and academic community already struggling to define 'terrorism', Kavanagh also noted how one company was attempting to overcome this hurdle by considering terrorist content to be any material posted by or in support of organisations included on the Consolidated United Nations Security Council Sanctions List. She also emphasized some of the challenges of dealing with the 'whack-a-mole' effect, whereby content taken down on one site is often reposted elsewhere, providing examples of how some companies are developing automated tools to scan, detect and remove terrorist content (notably images, audio and video) after it has been removed from one site.

Beyond the growing challenges of balancing security and rights in public and private responses to terrorist use of the internet and ICT, the authors questioned the effectiveness of existing approaches, noting in particular the absence of any mechanisms to assess their mid- to long-term effectiveness as well as the challenges in linking technology-based approaches to the deeper structural societal drivers of terrorism and violent extremism.

Lastly Carr discussed concerns relating to potential cyber attacks by terrorist groups against critical infrastructure, noting in particular how reference to the latter was included in the 2015 report of the UN Group of Governmental Experts on 'On Developments in the Field of Information and Telecommunications In the Context of International Security'. She also discussed a number of cooperative measures that are helping shape the response to existing vulnerabilities as a means to mitigate the threat.

Carr concluded her talk by reflecting on important challenges, including lacunae in international law relating to the protection of the global submarine fiber optic cable system through which 95 percent of global communications flow. The presentation left listeners with the nagging question of how the international community, already struggling to protect the simpler elements of information communication systems, can enhance and accelerate ongoing efforts aimed at protecting critical infrastructure from intentional interference such as terrorist attacks.

The Nature of States' obligations in the fight against cyber-terrorism

Dr Karine Bannelier, Université Grenoble-Alpes

Bannelier's presentation (delivered on her behalf by Prof Theodore Christakis) discussed the question of how responsible state behaviour should be defined in cyberspace, focusing particularly on the principle of due diligence. Bannelier explained that there is some debate as to whether the principle of due diligence applies to cyberspace. This debate stems from the use of the word "should" in reports produced by the UN Group of Governmental Experts. Bannelier argued that the word should be interpreted as meaning mandatory. She therefore drew attention to the 1949 Corfu case, in which it was found that a state has a general obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states. Territorial sovereignty entails not only rights, but also duties to other states.

Bannelier then considered the content of the due diligence principle. She argued that it should be interpreted as an obligation of conduct not an obligation of results. It should require that reasonable steps are taken: the level of diligence required should be proportionate to the dignity and strength of the power exercising it.

Bannelier warned against the 'unwilling and unable' test that was used by the US and UK as a justification for action in Syria. The 'unwilling and unable' test imposes an obligation of results over conduct upon the state in regards to non-state actors acting within its borders. To the extent that the 'unwilling or unable' theory was used in relation to the fight against terrorism and could, for instance, be invoked in the future in relation to cyberterrorism (or other malicious hostile actions by cyber-actors) it should be made clear that due diligence is not an obligation of result in addressing the consequences of a situation where a state is 'unwilling or unable' to ensure that its territory and critical infrastructures are used by non-state actors for harmful cyber operations against third states.

Bannelier then discussed when states have an obligation under the due diligence principle. Here, knowledge is key. Knowledge in this context includes constructive knowledge – which is important in the cyber domain where there are limits to actual knowledge.

Finally, Bannelier considered whether the due diligence principle extends to preventive steps. Although some states argue that the principle applies only to ongoing cyber operations, there is plenty of evidence that it is not limited in this way.

(En)Gendering Cyberterrorism in the UK news media: A discursive analysis

Dr Lee Jarvis, University of East Anglia

This paper explored how news media outlets portray cyberterrorism, and the importance of assumptions about gender within this. It drew on a wider empirical study with Stuart Macdonald and Andrew Whiting which investigated thirty-one news outlets within seven different countries, between the 1st January 2008 to 8th June 2013. Five hundred and thirty-five relevant items for analysis were taken from the dataset. With the data set amassed, two research questions were asked for this paper:

1. How is cyberterrorism given identity in news media discourse?
2. How is the discourse 'gendered'?

This paper examined how the news media portrays cyberterrorists and the threat of cyberterrorism in a very particular way. On the one hand, cyberterrorists are depicted as strong, resourceful, agential and determined. On the other, the 'self' that is threatened by cyberterrorism is widely presented as weak, ill-prepared and passive in the face of this threat. Nobody, it seems, is safe from this 'faceless' threat on the internet, and we are regularly warned about our dependence on digital architectures and technologies. These warnings are compounded by the widespread use of seemingly plausible hypothetical worst case scenarios.

The second part of the paper began by exploring how this construction of threat is implicitly gendered. The paper argued that the representation of cyberterrorists as resourceful, strong and determined relies upon longstanding assumptions about masculinity. The 'self' that is threatened, in contrast, is constructed in stereotypically feminine language: as passive and threatened. This is compounded, in news media coverage, by the focus on specific stories and pictures of 'dangerous' men, while women – when they are spoken about – are frequently spoken about as fragile and helpless victims, mothers or wives. It is very common in the media that masculinity is obscured when there is a need to invoke 'innocence' in a person. Demonising a person, on the other hand, often makes use of more stereotypically masculine constructs.

The paper concluded by exploring questions of authority and authorship within this news coverage. It showed that these news items are – overwhelmingly – stories that are (i) written by men, (ii) about other, often imaginary, men, (iii) heavily reliant on the authority of cited male 'experts', and (iv) illustrated by accompanying pictures of men and machines.

Cyberterrorism news media discourse, in short, produces this threat in a very particular gendered way.

The terrorist - hacker/hacktivist distinction

Leonie Tanczer, Queen's University Belfast

Tanczer started her presentation by highlighting that many hacker and hacktivist actions get entangled with (cyber)terrorism. However, no convincing data on their actual involvement in terrorism exists. Besides, the level of severity required for an act to be classified as cyberterrorism is contentious. Tanczer referred to a definition offered by Denning (2000) whereby cyberterrorism constitutes a serious attack against critical infrastructure and must cause enough harm to generate fear. Incidents that disrupt nonessential services or are mainly a costly nuisance would not. Based on this understanding, Tanczer criticised the comparison of hacking and hacktivism with cyberterrorism and used the conceptual ambiguity of these terms as a starting point for her analysis.

Tanczer's presentation was based on findings derived from her PhD thesis. In the course of this, she examined the understanding of hacking and hacktivism in the sphere of politics and industry, as well as amongst hackers and hacktivists themselves. She conducted interviews with self-identified hackers and hacktivists (n = 35) and used the results of this study to provide an overview of how this community actually perceives itself. Her presentation had two parts. The first examined assessments of hacking and hacktivism by external actors (e.g., politicians, the media etc.). This was done due to the fact that, in most cases, her participants would begin by responding to her questions by describing what others generally think of them. The second part then outlined the self-assessment of hackers and hacktivists.

One of the most profound findings of Tanczer's research was that interviewees argued that they are actively being criminalised. This is done through practices of instrumentalisation, which she defined as the purposeful attempt to construct them as a security threat. The hacker and hacktivist community would be faced with practices of Othering (e.g., comparison to 'modern folk devils'), dynamics of equation (e.g., equation with terrorism) as well as overestimations (e.g., comparison to cyberwarfare). Their construction as alleged "sociopaths" or "weirdos" would allow for their stigmatisation.

Tanczer also discussed her interviewees' views of their potential status within society (i.e., being beneficial and part of an 'eco-system') as well as their potential prosecution. She presented quotes from the interviews which highlighted the possible legitimisation of hackers and hacktivists and criticism of the harsh punishment of any form of computer misuse. According to her interviewees legal mechanisms should be in place that account for the diverse circumstances of a hack. This allowed for the fact that hacktivism is in many instances considered to be an online form of protest and civil disobedience. Interviewees also emphasised that there should be legal ways of being a hacker or a hacktivist.

Tanczer also urged caution about treating activism, criminal activities and terrorism interchangeably. She noted that we would never include offline activism, such as conducted by Greenpeace, with, for example, organised crime. Yet, it is commonplace to make such careless groupings in the online sphere. While we have legal protections for standing in front of a company or engaging in offline civil disobedience, its online equivalent is securitised and appears in online threat reports.

Tanczer finished her presentation by arguing for a shift of focus. Rather than automatically criminalising hacking and hacktivism, we should: (a) find a way to talk consistently about these phenomena; (b) engage and respond to these actions and actors sufficiently and appropriately; (c) begin a conversation about strengthening liberties online; and, (d) most importantly, allow research on the 'edges' of society to proceed. Only then will society be able to obtain a comprehensive assessment of such phenomena, including their potential security benefits).

Reality check: Assessing the unlikelihood of cyberterrorism

Prof Maura Conway, Dublin City University

Conway set out the argument, based on simple cost-benefit logic, that significant cyberterrorism attacks remain unlikely due to their high degree of difficulty and cost when compared to much more simple and commonplace means, such as car bombs. She pointed out that a lot of the research and commentary in this area focuses very much on technology, highlighting the fact that cyber infrastructures are not well secured. Globally, critical cyber infrastructures are vulnerable to attack by a whole range of actors; terrorists are not the ones we should be concerned about right now, she argued.

By way of a 'reality check', Conway's presentation compared the ease and low cost of Vehicle Born Improvised Explosive Devices (VBIEDs) or car bomb attacks versus cyberterrorism. The former have been used widely (e.g., Northern Ireland, Middle East, Sri Lanka, etc.) and with high levels of destructiveness. No act of cyberterrorism has ever yet occurred making comparisons difficult to carry out but, given, the attention to the cyberterrorism threat by media, policymakers, the Internet security industry, and others, nonetheless necessary.

Conway described four factors useful for calculating the probabilities of different types of terrorist attacks: cost; complexity; destruction; and, media impacts.

As regards cost: the 1993 World Trade Center (WTC) attack cost c.US$400. The Oklahoma City bombing killed 168 people in 1995 and cost about US$5,000. Estimates for the 9/11 attacks put the cost at about half a million US dollars. In 2006, the Pentagon put the average cost of an Afghan car bomb at US$1,675; the cost is unlikely to be greatly increased today.

With regard to complexity: many people worldwide have the know-how to construct VBIEDs. Reliable information about their construction is also accessible online. A major cyberterrorism attack, on the other hand, would require high-level technical knowledge that is not readily available to terrorists. The IT skills of violent Jihadis, for example, are not superior to those of the general public (although their PR department would have us believe otherwise), and hiring hackers to undertake such activity on behalf of a terrorist group could severely compromise the latter's security and has no guarantee of success.

On destructiveness: some of the obvious choices for a cyberterrorism attack – a hydroelectric dam or an air traffic control centre, for example – are not immediately attractive as they could much more easily be attacked using conventional means. Even if terrorists did manage to target the power grid somehow, we are more resilient than we think: power outages, even massive ones, occur frequently (e.g., due to fallen trees, faults, etc.) and nothing really happens.

Finally, media impacts are worthy of consideration: (live) moving images are crucial for truly spectacular terrorist events. There is no immediate theatricality in taking down a power grid or shutting down a water supply. Worse, from a terrorism perspective, the acts might be so low key as not to be considered terrorism or to be perceived or portrayed as accident or technology failure, etc. To claim such actions are still appealing to terrorists is to fundamentally misunderstand what terrorists want.

Comparing the relative ease, simplicity, low cost and high impact of car bombs with potential cyberterrorism attacks, both physically and in terms of media coverage, a cyber-attack does not seem a very appealing option for terrorists.

Weapons, wilderness and pathogens: investigating the techno-strategic language of the internet security industry

Dr Andrew Whiting, Birmingham City University

The primary interest of the paper was to investigate the manner in which cyber-threats were depicted by experts within a particular aspect of the cyber-security industry. Carol Cohn's 1987 study into defence intellectuals and techno-strategic language provided the theoretical lens through which this particular aspect of the internet security discourse was analysed.

The paper began by identifying the continued interest in nightmare scenarios within discussions surrounding cybersecurity and the tendency to speculate around a series of "what ifs?". Whiting equated this tendency to a "common sense" that has built up around the topic and argued that investigating cyber expert discourse is important to understand how this common sense has formed due to its powerful constitutive impact; a claim he sought to evidence with reference to notions of technification, security professionals and authorities of delimitation.

Whiting then elaborated on Cohn's study in which she gained access to a U.S. centre of nuclear strategy and while working alongside defence intellectuals observed the use of a particular language characterised as "techno-strategic". This language was heavily technified and included a prevalence of acronyms and metaphors that contributed towards a wider abstracting effect. This language had a significant framing effect, excluding, prioritising and organising the subject matter and with this in mind Whiting's research endeavoured to identify a similar language within the internet security industry. This was achieved via a discourse analysis of documents produced by a range of internet security companies between the years of 1997 and 2013, companies most commonly associated with the anti-virus products they produce (e.g. Kaspersky, AVG, Symantec).

Themes of vulnerability and destructiveness were evident within the discourse and manifested themselves prominently in a number of metaphors. Malware, for example, was synonymised frequently with pathogens and poisons in need of 'disinfection', while cyberspace itself was likened to the wilderness (a sort of cyber jungle full of predators and prey) or as a revisionist Wild West (anarchic, unruly, a sort Hobbesian state of nature). Destruction manifested itself through militaristic language and metaphor (i.e., weapons, arms race, cyber war, etc.). IT professionals became 'soldiers', 'warriors' or 'generals' while the malware itself were often characterised as 'bullets', 'bombs' and 'missiles'. Furthermore historic military metaphors were widespread with developments in cybersecurity likened to the Trinity tests, the Cold War, Pearl Harbour and 9/11.

Having established all of this Whiting posed the question of why any of this should matter to us? His response was that given the constitutive and productive power of discourse metaphors such as these serve to distil the complex into something more readily graspable and have an important role to play in the formulation of cybersecurity knowledge. This, in turn, can compound the seriousness, organises and prioritise responses and determines what is sayable and unsayable within debates on this area.

Whiting concluded by acknowledging how the metaphors identified here differ from those identified by Cohn, that instead of distancing the speaker from the actuality in this domain they serve to accentuate the threat. He also acknowledged the different role the internet security industry plays in comparison to the nuclear strategic centre Cohn focused on. The former of these sites having both a requirement to sell a product or products as well as communicate to a number of different audiences (including the public). Nevertheless, these companies still maintain expert status and further research should be conducted to explore this and other forms of cyber expert discourse as well as the intertextualities between these and policy and security discourses to illuminate the relationship that exists between them and the implications this has on resource allocation, policy and security practice.

Online Propaganda and Radicalization

Back to the Future: Online Propaganda and Radicalisation

Dr Alastair Reed, Leiden University

Reed began his presentation by stating that, when confronting the challenges presented by online content from the likes of al-Qaeda and Islamic State, there has been a tendency within the counterterrorism academic and strategic-policy fields to focus on what is new about this extremist propaganda. This results in it being portrayed as a unique threat, with emphasis being placed on the use of modern social media tools such as Twitter, Facebook and WhatsApp. This results in insufficient efforts being made to look at the past to see what lessons from can be learnt from history when responding to the contemporary threat. Reed's presentation therefore sought to place the current propaganda challenge into historical perspective and to identify crucial lessons learnt that are relevant to today's counterterrorism strategic communication campaigns.

Drawing on past communication campaigns from the American War of Independence, the Great Wars and the War on Terror, Reed argued that the evolution of propaganda in conflict has always been driven by three factors: developments in modern communication technology; advancements in military technology and strategy; and, the shifting relationship between the political elite and the populace. The struggle against AQ and IS propaganda should be understood in this historical context, from which lessons can be learnt for current counterterrorism strategic communication campaigns.

From this, Reed set out a framework consisting of macro, mezzo and micro level considerations. At the macro level, the considerations are reach, relevance and resonance. At the mezzo level, the considerations are medium, messenger and format. And at the micro level, the considerations are rational and identity choice appeals, defensive and offensive messaging (history shows that you need offensive strategic communications campaigns as well as defensive ones) and the say-do gap (there can't be a divergence between what you say and what you actually do).

Based on this framework, Reed set out four principles for the design of communication campaigns to counter violent extremism in the 21st century. There should be a diversity of messaging (rational and identity choice appeals, offensive and defensive messaging). There should a core theme (or grand narrative). A variety of media should be used. And strategic communications should be synchronised with political and military actions.

Predicting the Emergence of Self-Radicalisation through Social Media: A Complex Systems Approach

Prof Roger Bradbury, Australian National University

Bradbury began by stating the objective of his research: to predict the emergence of self-radicalisation through an empirical analysis of messages on social media. The approach is based on complex systems science. Underlying the study were three hypotheses regarding self-radicalisation. The first was that individuals reveal their 'identity' through their texts. The second was that self-radicalisation is a 'tipping-point' phenomenon, akin to a disorder/order phase transition where identity shifts rapidly from one metastable state to another. And third, an individual's identity will show critical slowing down prior to this change in state – the characteristic dynamics that predict the approach of a 'tipping-point'. The ambition of the study was to use complex systems science to create a data-driven real-time empirical analysis of the problem and to generate actionable predictions.

The first hypothesis is based on a forthcoming study which used a text analysis system called RPAS. Bradbury explained that the RPAS system uses indicators from a person's writing to create a stylistic signature. RPAS stands for Richness, Personal Pronouns, Referential Activity, Power and Sensory. Bradbury explained that it is possible to discriminate between individuals, and that identity is stable and consistent over time. Therefore, changes in identity can be related to major changes in the individual's psychological state. Indeed, in relation to the second hypothesis, it is possible to relate key points in a person's life to changes in their texts.

On the third hypothesis, Bradbury suggested that before a person is radicalised there will be a critical slowing down before the individual's thinking coalesces into a single unbreakable mind-set at the decision point. If it is possible to identify this slowing down, then the individual's change of state could be predicted.

Bradbury finished by explaining that the aim of his project is to identify a small population from a much larger population who are most likely to self-radicalise. Identifying this small population would allow agencies to focus their efforts more efficiently.

Prevention, anti-radicalisation and the role of social media: law enforcement agencies and their cooperation with other institutions

Dr Holger Nitsch, Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research, Germany

Recent terrorist attacks in Europe (both in Paris and Brussels) have brought into question why it is mostly young people who are influenced by radical ideologies. Nitsch suggested that with the spread of these ideologies, social media plays a very important role in regards to leading young individuals into believing radical and extremist ideas. He also suggested that even though social media is the main method of delivering these ideologies it can also be used as a counter measure, using the same persuasive techniques to promote de-radicalisation. The role of social media is exemplified in two case studies in Germany which were the focus of this presentation.

The term 'radical' in itself does not necessarily lead to extremism; as certain individuals who support movements such as animal rights, women's rights and racial equality can also be deemed radical, but perhaps not extremist. Nitsch depicted the process of radicalization in an individual as a pyramid, with the base being 'neutral' but rising to 'sympathizers, 'justifiers' and at the very top of the pyramid: 'personal and moral obligation' wherein a member feels like the ideologies of these radical groups become a moral obligation they must fulfil, the group is no longer a separate entity but converges with the identity of the individual. Nitsch went on to state that perhaps another reason as to why an individual may feel the appeal of these radical ideologies is due to a personal grievance they have suffered: extremist ideas then begin to act as a crutch for the personal grief. Due to the internet and the ease of publishing content, there is no end to where individuals can find ideas (forums, websites). With the array of social media platforms, the means of communication and exchange of conspiracy theory is very easy. This merely adds fuel to the already ignited fire in the individual and further persuades them to take on these beliefs.

Though some of the various methods of de-radicalisation prove to be effective, no 'perfect-method' has been found yet. This is understandable since persuasive methods of radicalisation have yet to be proven to be perfect – highly effective perhaps, but there is no fail-proof method to either type of measure. Nitsch explained that studies show that both the lone wolf ideology and recruitment techniques prove equally successful in the spread of radicalisation.

Radicalisers as Regulators: An Examination of *Dabiq* Magazine

Prof Stuart Macdonald, Swansea University

Macdonald's paper focused on the first 14 issues of *Dabiq*, the English language magazine published by the so-called Islamic State. The analytical framework he employed was the concept of responsive regulation. Macdonald conceded that at first there appear to be dissimilarities between this concept – which was devised by Ayres and Braithwaite as a contribution to debates on business regulation – and the production of jihadist magazines. However, he explained that regulation is not the sole preserve of the state – private actors can also regulate responsively – and regulatees may include individuals. Indeed, Braithwaite himself later applied the concept of responsive regulation to convicted offenders. The reason for employing responsive regulation as the analytical framework for this study was that, like attempts to radicalise, the aim of responsive regulation is to secure compliance with a set of norms by achieving attitudinal and behavioural change. Research into responsive regulation therefore offers the opportunity to gain fresh insights into radicalisation processes.

Macdonald also explained that there are stark difference between the norms which business regulators seek to impose and those advocated by the producers of *Dabiq*. The norms enforced by business regulators are based on the current, physical world, whereas the norms advocated by the producers of *Dabiq* are based on the spiritual, as well as the physical, realm and on the hereafter as well as the here-and-now. This point is key to understanding the coercive power which the so-called Islamic State may potentially wield over those who live outside geographical areas under its control.

Macdonald went on to outline the variety of persuasive techniques which *Dabiq* uses to regulate its readers, including presenting the benefits of adherence to IS (both physical and spiritual), emphasizing religious duty and warning of punishment. Macdonald explained that biographies of those killed in performance of jihad are frequently used to reinforce the promise of future spiritual benefits.

One of the key features of responsive regulation is the way in which the various regulatory techniques are organised into a regulatory pyramid. Regulators begin at the base of the pyramid, attempting to coax compliance by persuasion. If this fails there follows escalation to the more coercive strategies higher up the pyramid. This avoids the negative psychological impact of immediate recourse to punishment which projects negative expectations onto the regulated actor. It also achieves a synergy between persuasion and punishment; regulatees are more likely to engage with persuasive techniques if they believe escalation in the event of non-compliance is inevitable. Macdonald explained that *Dabiq* presents future punishment as certain for those who do not act upon its call to jihad. Moreover, it presents the threat of punishment as emanating not from itself, but from Allah. Similarly, regulators depict the threat of future punishment as emanating from outside third forces as this helps construct relationships of trust with regulatees.

Macdonald concluded by highlighting the emphasis *Dabiq* places on procedural fairness in its accounts of executions and punishments. Social justice research indicates that judgments about procedural fairness are as important as judgments about substantive fairness (if not more so). Indeed, *Dabiq* frequently juxtaposes the actions of IS with those of Western governments, which are depicted as unjust both procedurally and substantively. This technique is used to consolidate sympathisers' willingness to self-identify with the in-group (IS) and distance themselves from the out-group (the West).

(De)legitimation in Terrorist Narratives: A Corpus-Assisted Discourse Studies Perspective

Prof Nuria Lorenzo-Dus, Swansea University

Lorenzo-Dus' paper began by contesting the claim that the current supposed stagnation in the field of terrorism studies is due to an over reliance on the study of terrorists' messages (i.e., their discourse). The aim of her presentation, she explained, was to offer a better understanding of how discourse analysis should be conducted and the potential value of such an approach by presenting the findings of a case study of the online jihadist magazines *Dabiq* and *Inspire*.

Lorenzo-Dus explained that Corpus Assisted Discourse Studies (CADS), the discourse analysis method she used, is centrally committed to linking textual features to social practices. Its aim is to uncover non-obvious meanings; that is, meanings which might not be readily apparent to the naked eye. Having uncovered these non-obvious details through quantitative, software enabled tools, CADS then aims to explain and interpret them through qualitative linguistic analysis and insights from relevant non-linguistic disciplines. CADS follows an inductive approach which revolves around identifying frequency based lexical patterns within large corpora. While this does not remove subjectivity entirely from the analysis, it does make the analytic steps taken to identify these patterns replicable and accountable.

Lorenzo-Dus then presented her case study. This focused in particular on the language used to de-legitimize 'the West' and legitimate jihadist ideology groups' violence against 'non-believers' in Al-Qaeda's magazine - *Inspire* - and the magazine of the so-called Islamic State - *Dabiq*. The study was guided by three propositions.

First, religion plays a pivotal though controversial role within jihadist ideology, which is based on a modified version of the Islamic idea of da'wa. Da'wa traditionally consisted of peaceful missionary work but this has been subverted in its current usage as a justification for killing non-believers. Second, jihadist ideology is based on polarised argumentation. There is no middle ground; those in favour of jihad are glorified, those against are vilified. Third, jihadist groups are not homogenous. Al-Qaeda believe in targeting the far enemy before the near while Islamic State focuses first on the near.

The results of the study offer insights into how *Dabiq* and *Inspire* used different verbal attacks (impoliteness strategies, in linguistics) to delegitimise the West. *Dabiq* favoured the use of scorning and ridiculing, mainly targeted against Western leaders; *Inspire* favoured the use of distancing, primarily on religious grounds. The study results also showed that the two magazines used similar grounds when seeking to legitimise their violent acts against 'non-believers', especially those they labelled 'kuffar' and 'murtaddin'. These combined 'impersonal authority' legitimation (that is, legitimation through religious law, rules and regulations) and mythopoesis (i.e., legitimation through narratives in which online jihads were portrayed as saviours).

Militant Islamist propaganda targeting Muslims in the West: Comparing *Inspire* and *Dabiq* narratives

Dr Haroro J. Ingram, Australian National University

Ingram presented the findings of a comparative study of the so-called Islamic State's magazine *Dabiq* and Al-Qaeda's magazine *Inspire*. His paper sought to explain how *Inspire* and *Dabiq* attempt to appeal to and radicalise English-speaking Muslims through the use of strategically designed in group, other, crisis and solution constructs which are variously interplayed through the use of value, dichotomy and crisis reinforcing narratives. While acknowledging the tendency for Western foreign fighters and 'lone wolves' to consume propaganda from both Al-Qaeda and IS, Ingram used *Inspire* as a comparator to *Dabiq* to offer insights into how and why IS supporters seem to radicalise more quickly.

Ingram explained that, whilst *Inspire* is dominated by identity-choice messaging (i.e. appeals designed to coax audiences into making decisions based on identity), *Dabiq* balances identity-choice messaging with rational-choice messaging (i.e. appeals designed to lure audiences into making decisions based on a cost-benefit consideration of options). Regarding the latter, *Dabiq* presents reports of IS's pragmatic actions that are contributing to security, stability and livelihood for populations under its control. This form of messaging is designed to compel its audience to engage in rational choice decision making, that is, decisions based on cost benefit consideration of options.

At the same time as compelling rational choice decision making, *Dabiq* also proclaims messages that draw on perceptual factors, i.e., IS's 'cause' particularly pertaining to its ideological contentions. These messages are designed to present IS as the champion and protector of Sunnis - the in-group identity. This formation simultaneously portrays IS's enemies as being responsible for all the crises befalling the Sunni population. This form of messaging compels *Dabiq*'s audience to engage in identity choice decision making. Ingram emphasised the importance of Othering and in-group construction.

Dabiq's messaging is designed to fuel the process of cyclical cognitive reinforcement. As the in-group is portrayed as benevolent and responsible for solutions, and as an increasing number of crises are attributed to the in-group's enemies – the Other – a self-reinforcing cycle emerges.

Ingram concluded by outlining some key lessons for counterterrorism strategic communications from his analysis. The primary lesson was that counterterrorism strategies should avoid reinforcing the bifurcated worldview of violent extremist groups such as IS and Al-Qaeda. Messaging should instead be focused on two core themes designed to address rational and identity choice decision-making processes. To address identity choice issues, counterterrorism strategic communications should highlight the range and diversity of identities rather than reinforce the bifurcated worldview of extremists. This should be part of a broader approach that seeks to reverse IS's playbook. Counterterrorism strategic communications messaging should therefore seek to depict IS as the source of the Sunni population's problems and western governments and allies as sources of practical solutions. Additionally, this messaging should always aim to highlight and accentuate the gap between what IS says and does while diminishing its own say-do gap. This approach is designed to not only boost the effects of politico-military/counterterrorism actions but disrupt the process of cyclical cognitive reinforcement in the favour of extremists.

In search for those who loose and bind: Views from al-Qaeda on how to appoint a caliph

Dr Gunnar J. Weimann, independent researcher

The aim of Weimann's paper was to present an overview of al-Qaeda's responses to the events of recent years: namely, the Arab Revolutions, increased use of social media and the rise of the so-called Islamic State. The first part of his presentation outlined al-Qaeda's change in strategy following Ayman al-Zawahiri's ascension to the leadership of al-Qaeda in 2011. In particular, Weimann discussed two documents produced by al-Zawahiri in 2012 in response to the popular revolts: his *Document in support of Islam* and his *General Guidelines for Jihad*. In these documents, al-Zawahiri defines a new strategy for al-Qaeda: al-Qaeda should merge with the population, cooperate with other jihadist and Muslim groups, avoid conflict with local regimes where possible and try to take control of territory to be used as safe havens, from which it can prepare attacks against Western targets. The ultimate aim of this new strategy would be the creation of a "rightly guided" caliphate, which would ensure political unity, participative governance, justice and welfare for Muslims.

Following the publication of these strategic documents, the three major al-Qaeda affiliates, al-Qaeda in the Arabian Peninsula (AQAP), al-Qaeda in the Islamic Maghreb (AQIM) and Jabhat al-Nusra, implemented this strategy, which seemed to yield important successes in the beginning. These gains were placed in jeopardy by the unilateral declaration of the caliphate by the Islamic State (IS). Weimann argued that the conflict between IS and al-Qaeda was not only about the leadership of the global jihad movement. The behaviour of IS, in particular the declaration of the caliphate, contradicted al-Qaeda's new strategy to an extent that al-Qaeda had no other option than to expel IS from the al-Qaeda network. In addition, the declaration of the caliphate by IS forced al-Qaeda to develop more concrete ideas about how a "rightly guided" caliphate could be achieved.

Traditionally, a caliph can either be elected or appointed by a predecessor. Both options require the approval of a group of people known as the *al-ḥall wal-ʿaqd* ("those who loose and bind"). Based on an analysis of four ideological treatises published by AQAP, AQIM and Jabhat al-Nusra, Weimann explained how al-Qaeda attempted to address popular demands in the wake of the Arab revolts by promising increased opportunities for political participation in the establishment of the caliphate by emphasising that the *al-ḥall wal-ʿaqd* must represent the entire Muslim community. However, the challenge al-Qaeda faced in doing so was not to appear to be advocating democratic rule, given that salafism rejects democracy as irreconcilable with Islam.

The resulting new al-Qaeda discourse on the caliphate might not be a consistent political theory, but it might enable al-Qaeda to win support with a political project appealing to audiences beyond the closed circles of jihadists and to cooperate with forces that do not necessarily subscribe to its global jihad ideology.

In summary, the paper showed that the advent of social media and the ensuing increased possibilities for popular mobilisation changed not only the way in which terrorist groups such as al-Qaeda communicate but also the messages addressed to different audiences and the strategies of terrorist groups to relate to local populations. Such changes, however, do not entail a fundamental change in the overall ideology of al-Qaeda, which continues to consider Western countries and interests as its main targets.

Online Finance

Online Terrorism Financing

Burke Basaranel, Swansea University

Basaranel described the similarities between the criminal world and terrorism financing. Though he did not give figures of money transferred online through untraceable means such as pre-paid cards and through unregistered charities, it was clear that these are popular due to the speed and anonymity such means can provide. Basaranel described terrorist organisations' online fundraising to be both a means of raising finance as well as propaganda, and divided the funding methods of terrorist organisations into passive and active methods according to the level of coercion of fundraisers and consent of donors.

Basaranel explained that the creation of unregistered charities as a means to launder money has long been a method utilized in the criminal world and is now one employed by terrorist groups as a means of funnelling money and raising funds in a consensual manner. Moreover, he explained that the benefit of using unregistered charities is that they are easier to source revenue for.

In regard to active methods of online terrorist funding Basaranel described the utilization of pre-paid cards. The key feature of pre-paid cards is that they are not tied to an identity but rather just a randomly generated code. Pre-paid cards can be used to fund terrorist attacks and operations without detection via a simple chain of actions. A terrorist organisation would ask a supporter via, for instance, Skype to purchase a voucher from Apple or Amazon and then send on the voucher code. The voucher code would then be sold online for less than the voucher's value in return for cash which would go into an account registered to a terrorist organisation or actor.

Though pre-paid cards and unregistered charities make the money trail difficult to follow, terrorist organisations do not yet use virtual currencies such as Bitcoin with the same frequency as criminal organisations and have yet to progress fully to more encrypted forms of money transfer. So, whilst Basaranel suggested that there should be some form of monitoring of the means he had described, the danger with aggressive policies is that they could coerce terrorist groups into using methods which are more difficult to track.

Cybercrime-funded terrorism and the threats posed by future technologies

Ltn. Col. Gianluigi Me, Deputy Head of ICT Security Department, Italian Carabinieri; **Maj. Giovanni Bottazzi**, Head of Network Security, Italian Carabinieri

Bottazzi and Me's presentation focused on cybercrime and its links to terrorism funding, describing the 'crime as services model'. The presentation also gave examples such as the shutting down of nuclear plants and power grids to highlight the potential for cyberterrorism.

Bottazzi described the prominence and rise of cybercrime. Last year was described by Bottazzi as 'The Year of Collateral Damage'. The Internet's economy generates approximately 3 trillion US dollars a year from which cybercrime garners 15-20%, around 400 billion US dollars. With 50% of people shopping online and 40% banking online there is access to real money provided that you can find a software's vulnerability – which, according to Bottazzi, every software has. The near-guarantee of money and high revenues per action make renting high-tech tools to infiltrate software very attractive to terrorist organisations that may not have the technological knowhow.

Bottazzi presented a grim outlook for the security of money and information online. However he did describe bug bounty programs, which expand a company's recourses affordably, to discover the weak points in software. Bottazzi emphasised the importance of increased security online because, as he expressed it, "We are no longer individuals but are data clusters". Time and funding should be invested in finding and resolving, for instance, online banking websites' weak points. However there are tensions here. First, new website operators generally want to get their new system out as quickly as possible to beat the competition. And, second, weaknesses in the software and user-friendly operations often go hand-in-hand, so to fix a bot that has been discovered may hinder the slickness of a site.

Cyber Surveillance

Privacy versus security in the cyber-surveillance debate

Sergei Boeke, Leiden University

Boeke's presentation began with an overview of the effect the Snowden revelations have had on backdrop surveillance. Prior to June 2013 the US media were often reluctant to report on NSA surveillance practices due to government pressure. After the revelation of these surveillance programs by Edward Snowden, many of the NSA's activities were framed as "mass surveillance". Not all of the NSA's programs should, however, have been seen as mass surveillance and several leaked slides were taken out of context and subject to misinterpretations. As a result of the revelations there was an internet wide increase in the use of encryption, a shift in business away from US IT companies and a chilling effect on internet behaviour.

The presentation continued with a discussion of the nature of surveillance, privacy and anonymity. Surveillance, or the garnering of data for detailed analysis, was defined as the systemic monitoring of people without discriminants. The obvious conflict with privacy was broached, and while it was conceded that the definition of privacy is contextually and culturally dependent it can generally be said to be the right to have control over one's personal information. It is a basic human right and essential for a free and democratic society. While EU data protection laws exist to protect privacy, these are only applicable to the private sector. The European Convention on Human Rights does constrain governments that are party to the treaty, and there is considerable jurisprudence on surveillance and espionage.

The question of anonymity was discussed by Boeke who argued that to be anonymous is to be unidentifiable in one's actions. Unfortunately there is very little jurisprudence in regards to the right to anonymity and contrary to this concept many states have compulsory ID laws. Metadata collection is an interesting case to further examine as in many cases the records remain anonymous, and are not coupled to identities. Once an investigation focuses on a particular contact or record, however, anonymity can quickly be lost, with potential implications for the privacy of the individual concerned.

The remainder of Boeke's paper consisted of a series of comparisons. The distinctions between domestic law enforcement approaches and intelligence agency approaches were discussed, where domestic law enforcement tends to favour targeted, downstream data collection (direct acquisition from an Internet service provider) focusing on content. On the other hand, intelligence agencies, faced with the task of collecting data abroad, tend to favour upstream bulk collection of metadata and content. The differences in operation of three US surveillance programs – PRISM, Stellar Wind and the Mystic Program – were then discussed in terms of data collection, analysis and targeting. The most important distinctions when looking at surveillance programs is whether the collection is at home or abroad, and whether they target individuals (select and then collect) or collect in bulk (collect and then select).

National Security, Cyber-surveillance and International Law

Prof Theodore Christakis, Université Grenoble-Alpes, Institut Universitaire de France

Christakis' presentation began by outlining the tension between, on the one hand, the consistent use of national security arguments by governments to justify the creation of new laws, caveats and exceptions, and, on the other hand, the danger that if governments could not do this they might not engage with international law. Against this backdrop he then introduced the new French law on surveillance. This has two strands: domestic surveillance and international surveillance. Christakis' focus in this presentation was domestic surveillance. He explained that the French Government offered a range of justifications in support of the new law, including mainly the prevention of terrorism.

Christakis then outlined the techniques and methods used by the new law, which opponents have described as a "French Patriot Act" and a major blow to human rights, as well as constraints on its use. He explained the role of the Commission (CNCTR), which has control functions both *a priori* and *a posteriori*.

Christakis explained that this law is now facing international legal challenges, including several applications lodged with the European Court of Human Rights (ECtHR) by journalists and lawyers. He then examined the existing case law of the ECtHR starting with procedural issues, specifically, the admissibility of applications. Here two issues in particular were discussed; the victim requirement and the exhaustion of domestic remedies. In terms of the victim requirement, the difficulty faced by individuals wishing to bring a claim under Article 8 ECHR is establishing that they are under surveillance, since the surveillance programmes are secret. However, according to the ECtHR in *Klass and others v Germany*, "an individual may under certain conditions, claim to be the victim of a violation occasioned by the mere existence … of legislation permitting secret measures, without having to allege that such measures were in fact applied to him".

Christakis then considered a series of substantive issues. These included the questions whether there had been potential interference with the applicant's rights, whether the restrictions were "prescribed by law", whether they pursued a legitimate aim, and whether they were necessary in a democratic society. The latter requires an assessment of necessity, proportionality and consideration of existing safeguards.

Christakis ended by pointing out that the ECtHR has struck down the surveillance laws of several states in recent years, and reiterated the importance of legal safeguards such as Article 8 ECHR against state misuse of surveillance and other investigative powers.

Beyond big data: surveillance, metadata and technology-enabled intelligence opportunities in counterterrorism

David Wells, former Intelligence Officer at GCHQ, the Australian Signals Directorate and the Australian Crime Commission

Wells began his presentation by highlighting recent technological developments which mean that, in 2016, intelligence agencies have potential access to more data, and more types of data, than ever before.

Although it is difficult to assess intelligence agencies' use of big data in counterterrorism, Wells identified three key terrorism trends since 2012 that point towards the potential benefits of using big data in this way. Modern terrorist groups are bigger in both size and scale, operate transnationally, and rely on data-generating technology.

These trends have implications for counterterrorism investigations. First, many agencies are faced with more intelligence targets than they can monitor effectively in a targeted and intensive way. Second, although the terrorist threat is transnational, many intelligence agencies currently have a narrow, predominantly domestic focus. And third, technical intelligence collection options are not only likely to be more effective than their alternatives, they are also less risky. Wells argued that because of these trends, intelligence agencies can no longer solely rely on traditional intelligence gathering methods. Instead, he advocated that they be supplemented by a big data approach.

Such an approach is not without its own challenges, foremost of which is the rise of widespread encryption. This, combined with moves by communications companies to transmit and store their data in a manner that is difficult for intelligence agencies to access, makes getting hold of big communications datasets challenging. And once accessed, the agency must be able to store, process and analyse the dataset in an effective and efficient way to ensure that they derive intelligence value.

Wells then outlined an example case study of how this might work in practice, demonstrating that rather than trawling through large datasets in a manual fashion, intelligence agencies search for multiple elements or patterns of behaviour. This results in intelligence analysts looking at a small, filtered subsection of the big dataset, containing data largely relevant to their intelligence requirements.

He further identified two key advantages of such an approach: speed, and the ability to identify individuals of interest and their communications devices. In the current terrorist and communications environment, big data can deliver unique value to intelligence agencies.

The paper concluded with an assertion by Wells that data collection is just the first part of the counterterrorism intelligence process. The collected data must be interrogated through the use of smart, focused questions, whether algorithmic or analyst-driven. Big data methods provide unique value but they should only supplement other intelligence collection methods. In order to be successful, intelligence agencies must combine these methods with intelligence-sharing partnerships at both national and international levels.

Responding to Terrorists' Use of the Internet

Terrorist use of the internet and regulation of online content

Francesca Bosco, UNICRI

This paper provided an overview of the debate around responding to online terrorist content, evaluating the different options of suppression, regulation and engagement. Traditionally, it was easier to distinguish between official terrorist websites and accounts and unofficial ones (even if this could sometimes be challenging). Now with the prolific use of social networks there is a blending of official and unofficial activity. Another issue is the instantaneous nature of modern social media. The live tweeting of the capture of Mosul by Daesh forces in 2014 was given as an example. A further challenge facing efforts to enforce restrictions on terrorist content on Twitter, Instagram, etc., is the fact that the propaganda is being disseminated and filtered by unwitting users as well as supporters.

The UN has attempted to develop a balanced counterstrategy. Its 2006 Global Counter-Terrorism Strategy included ideas and goals aimed at denying terrorists access to their audience. Whilst suppression has been the dominant approach thus far, it is a strong form of response and has had mixed results. Taking child pornography as an example, there are serious problems with attempting to simply shut things down the moment they surface.

Bosco also identified a definitional problem; there is a lack of international understanding and agreement when it comes to online terrorist activity. Furthermore, even if there was unanimity in terms of a definition, from a practical point of view law enforcement capabilities vary widely worldwide.

The suppression approach has seen disproportionate knee-jerk suggestions, such as switching off satellites or even chopping cables. Efforts at suppression are likely to prove ineffective for many reasons, not least the fact that if you shut down activity in one place it will almost immediately pop up somewhere else. Generally, there is strong public opinion against filtering; it fundamentally conflicts with freedom of expression. It also raises the question of content responsibility: who sets the criteria for removing material? Even if these questions could be answered the regulations would be difficult to enforce as there is nothing approaching a centralised control over the internet, nor should there be. On the one hand, if a service provider becomes aware of extremist content it would be unethical not to act; but on the other hand, would people generally be happy to have their entire internet experience monitored?

The Council of Europe has stated that any restriction of user content must be based on a strict and predictable legal framework: a situation that does not exist in most countries. A comparative assessment study conducted by the Council into filtering, blocking, or removing information found that most countries do not have specific legislation dedicated to this issue. Instead other legislation is leveraged into action. The EU itself is unlikely to witness knee-jerk blocking actions due to the protections of Article 10 of the ECHR but there are still tensions, especially between law enforcement and the private sector. It is noteworthy that EUROPOL has recently established an EU internet referral unit which is now fully operational and facilitating cooperating with the private sector. The European Commission and several IT companies have also recently announced a code of conduct that applies to online hate speech. This illustrates that public institutions are beginning to find ways to engage with the private sector. Both hard and soft measures (from removal procedures to raising awareness among users) are being employed. But, Bosco concluded, further debate is needed in order to clarify the rules that are emerging and to ensure an appropriate balance is struck.

Prosecuting terrorist activity in Canada

Angela Gendron, Carleton University

Gendron's focus was the criminalisation of terrorist activity in Canada, in particular the use of precursor offences to prosecute those involved in terrorist-related activities as a pro-active preventative legislative counter-terrorism measure.

Gendron began by identifying the central tension between criminalising those terrorist-related activities that can reasonably be considered 'acts preparatory' to a serious future attack and the intention of the courts not to punish "individuals for innocent, socially useful or casual acts which, absent intent, indirectly contribute to a terrorist activity." As defined in Canada's Criminal Code, the facilitation of terrorism does not require the accused to know whether "any particular terrorist activity" has been planned; it is sufficient to prove beyond reasonable doubt that he had knowledge and intent to facilitate a terrorist activity. Proving intent can be problematic but in prosecuting offenders, there is considerable judicial discretion to tailor the sentence to the particular circumstances and the harm entailed.

After providing an overview of the Canadian definition of terrorism, Gendron provided examples of the precursor offences contained in the Canadian Criminal Code. These included: participating in the activities of a terrorist group; facilitating terrorist activity; instructing anyone to carry out terrorist activity for a terrorist group; travelling abroad to commit a terrorist act; and, financing terrorism. A new offence created by the Anti-Terrorism Act (2015) makes it a crime for any person "who by communicating statements, knowingly advocates or promotes the commission of terrorism offences *in general*," punishable by up to five years' imprisonment. The Act also includes provisions for the seizure, and online take-down of terrorist propaganda and reduces the qualifying criteria for preventative recognizance (peace bonds).

Gendron then provided examples of the issues which had surfaced in the trials of those who had been prosecuted in Canada for terrorist-related activities since 2004. In *R v Khawaja*, a Supreme Court ruling found the 'motive clause' in Canada's definition of terrorism did not infringe freedom of expression and therefore did not violate the *Charter of Rights and Freedoms*. It also affirmed the constitutionality of Part II.1 (Terrorism) of the Criminal Code in terms of the scope of the law. In *R v Namouh* the prosecution case focused on Namouh's intent in making and disseminating videos for the Global Islamic Media Front, while the case of *R v Ahmed* provided an example of how proactive prosecution for precursor activities can prevent the accused from proceeding towards more serious terrorist acts. *R v Thambaithurai*, was the first conviction in Canada for financing terrorism: the prosecution's task was to demonstrate the accused's intention to finance terrorism by establishing the connection between the World Tamil Movement, for which he raised funds, and the Liberation Tigers of Tamil Eelam – a listed terrorist organization.

Gendron concluded by referring to the case of John Nuttall and Amanda Korody, found guilty of planning to detonate pressure cooker bombs at British Columbia's legislature on Canada Day. Sentencing has been put on hold while an allegation of 'entrapment' is considered. Gendron used the case to flag concerns that the need to prevent attacks had led to early interventions which can deny law enforcement vital evidence. As a consequence, undercover agents are increasingly being used (especially in the USA) to ascertain the intentions of suspect individuals/groups. In some cases, the actions of these agents may cross the boundaries from information gathering to instigation. For example, an undercover agent was a key prosecution witness in the trials of members of the 'Toronto 18' home-grown terrorist cell.

Interrupting Engagement with Online Extremist Content: Utilising 'Noisy' Foreign Fighters

Dr Jamal Barnes, Edith Cowan University

Barnes began by explaining that, whilst there has been a large amount of attention paid to CVE strategies that seek to remove online content, these strategies will only be effective if used in conjunction with counter-narrative strategies. Counter-narrative strategies go beyond removal strategies by employing the use of physical and psychological noise to drown out extremist online content.

Against this backdrop, Barnes presented research carried out by the Countering Online Violent Extremism Research Program, Exit White Power, the Institute for Strategic Dialogue and the Richardson Peace Institute. This study examined the response of the audience to "discussion" starters about extremist topics in public online forums as well as one-to-one engagements with social media. They found that social identity was integral to understanding why individuals engaged with violent extremist content. In line with this, counter-narratives that focus on identity rather than rationality (facts and figures) generated more of a response from users. Furthermore, shared experiences about violent extremism generated similar results as did including civil society in the discussion.

Barnes then used this importance of identity and shared experience to begin his justification for rethinking the problem of foreign fighters. In order for counter-narratives to employ the use of foreign fighters, efforts must be made by governments and legal systems to move beyond prosecution as the only option of dealing with a returning foreign fighter. One step suggested by Barnes was to place foreign fighters on a sliding scale of threat instead of treating all of them as dangerous terrorists. One example cited was of Denmark who have both a law enforcement and rehabilitation approach where foreign fighters wishing to return have been repatriated and offered employment and treatment for injuries.

The reasons why foreign fighters should be used in counter-narratives, Barnes explained, are multiple. They have first-hand experience of the narratives which compel people to join extremist groups, and their abandonment of these narratives and groups means that they offer a credible voice which government-led counter-narratives usually lack. Moreover, foreign fighters can speak with authority about the conditions on the ground under ISIS. One of the biggest pull factors in ISIS propaganda is the promotion of a life of 'pure Islam' under the Caliphate. Returning foreign fighters from ISIS territories can be indispensable in dispelling this myth. They can speak about how initially they were drawn to the idea of the Caliphate but became disillusioned when faced with sexual violence and other violent acts, as well as the killing of innocent Muslims by ISIS. And, in addition, returning fighters also have access to radicalised networks in their country of origin and can help advance understanding of the motives behind would-be foreign fighters.

Barnes concluded his presentation by discussing the link between counter-narratives and the offline world. Returning foreign fighters are not a silver bullet for efforts to counter online terrorist propaganda. In order for counter-narratives to be effective we must look to our own actions in the West and how these may be at odds with the narratives we present about ourselves. We must avoid giving terrorists and extremist organisations ammunition in the form of Western hypocrisy. Closing the gap between online narrative and offline activity is key to countering online terrorist propaganda effectively.

Hard and Soft Approaches to Countering Online Extremism

Dr Keiran Hardy, Griffith University

Hardy began his presentation with a discussion on the nature of hard and soft power. Hard power is the capacity to influence behaviour through direct coercion, threats and inducements, whilst soft power is the capacity to influence behaviour through the attractive power of culture, ideology and institutions. Hardy then introduced Joseph Nye's notion of smart power. This is where hard power and soft power are used in combination in order to develop strategies which are effective in varying contexts. He then applied the notion of smart power to the counterterrorism context. This is appropriate given that the UK's CONTEST strategy calls for effective security measures, intelligence and policing whilst simultaneously placing equal weight on tackling the social factors underlying radicalisation.

One problem with this active use of both hard and soft power is that it results in situations where both may appear to be applicable at the same time. Hardy outlined several possible situations where a choice would have to be made between either a legal (hard) or policy (soft) response. For example, what is the appropriate response to a person who accesses, reads, downloads and prints extremist and instructional materials posted on the Internet? What is the appropriate response if this same person shows these materials to others at a local mosque, telling them they should decide for themselves whether to support Islamic State?

This led to a discussion of the UK Government's *Channel* initiative, the aim of which is to protect vulnerable people from being drawn into terrorism. The risk factors which *Channel* uses for determining whether individuals are vulnerable to radicalisation often overlap with terrorism precursor offences which target the possession of materials associated with an extremist cause and supporting violence toward others. A difficulty with this overlap, Hardy continued, is that the close relationship between hard and soft power approaches to counter-terrorism creates damaging perceptions of surveillance and discrimination in Muslim communities. It leads to claims that work aimed at preventing violent extremism is merely a pretext for surveillance and that those delivering community projects are no more than police spies.

The presentation concluded with some recommendations for governments moving forward. In particular, Governments need to signal in clear terms what forms of online conduct are: (1) potentially unlawful and will trigger criminal investigation and prosecution; (2) not unlawful but provide evidence of extremist beliefs and a risk of terrorism, and may therefore trigger a targeted intervention or de-radicalisation program; and, (3) legitimate forms of speech that should be supported in a free, democratic society.

Threat Assessments and the Internet

Dr Paul Gill, University College London

Gill's presentation outlined several problems in the scientific study of risk factors of radicalisation. First, the literature consistently identifies more and more risk factors – many of which are empirically questionable and difficult to operationalise. Second, the study of these risk factors also tends to weight them all equally. Building a bomb and being interested in foreign travel are both considered equally worrying terrorist indicators in some publications. There is currently no sophisticated way of weighting the indicators. Third, we have no idea of base rates when it comes to indicators. Fourth, current studies typically tend to treat all terrorists equally. Bomb makers and bomb planters have very different motivations and behaviours. 'Who becomes a terrorist?' is a terrible question; there are lots of subcategories within terrorism and we need to be more specific. Criminology learned this a long time ago but terrorism studies has been slow to follow suit. And fifth, we have very little understanding of protective factors.

The risk assessment of online radicalisation specifically throws up an additional couple of problems. First, many people project false images of themselves on online social media platforms. This is true for both benevolent and malevolent individuals. Our abilities to tell what is actually true are made more difficult when viewing these online behaviours at a distance. Second, there is a huge proliferation of extremist material. Analysts are simply drowning in data. There is therefore a great need for helping them triage the types of behaviours they need to be looking for.

Terrorists use the internet in many different ways. In one of Gill's studies, he found that lone-actor terrorists use the internet to learn (about issues like ideology, the need for violence, target choice, target choice, attack preperation and how to overcome hurdles they face) and to communicate (on reinforcing beliefs, seeking legitimisation, disseminating propaganda, attack signaling and recruitment). In a follow up study funded by VOX-POL, Gill et al., studied the online behaviours of 227 UK terrorists. Gill's study found that extreme right wing terrorists were 3.5 times more likely to learn online than jihadis. However this is not surprising as the extreme right wing terrorists were most often lone actors with no support networks. The study also found that those targeting high value targets were more likely to conduct online research. Those using IEDs were 3.34 times more likely to learn online. Lone actors were 2.64 times more likely to learn online than cell members. The results therefore show that different types of terrorists and terrorist attacks will leave a significantly different online footprint from one another.

Gill concluded by suggesting that the major focus on preventing radicalising material is perhaps misguided and that a greater focus should be placed upon the materials that provide specific practical guidance on how to conduct a terrorist attack. The solution is to minimise opportunity for violence rather than countering extremism itself.

Anglosphere approaches to counterterrorism policy in cyberspace

Dr Tim Legrand, Australian National University

Increasingly states are facing threats that span borders, domestic and international problems are blurred and policy makers are much more attuned to transnational threats. The dilemma is that the state has been contracting in terms of powers and capacities. It has been hollowed out in favour of the private sector and civil society. The state is expected to do more with less.

What do these challenges look like in the Anglosphere? (Not the neo-con version: saving good of the world – though analytically it works well). In his presentation Legrand examined the relationship between Canada, the UK, the USA, Australia and New Zealand. These countries share some very strong historical and cultural heritage and have a significant history of military alliance. Their 'WASPishness' (White Anglo Saxon Protestant) is shared. The Westminster system, with the exception of the United States, has travelled. With common law, similar ideas around democracy, mercantilism, capitalism, and state infrastructure these five countries see themselves in each other.

All have experienced extensive privatisation of critical infrastructure so are facing similar security challenges. Since the 1990s 23 policy networks have been established between heads of departments or Ministries that involve physical participation. The problem is that researching security policy is extremely difficult; there is lower transparency and fewer accountability mechanisms. However, there is a distinct pattern of collaboration in the Anglosphere; there has been significant security engagement especially since 2009.

The Five Eyes relationship developed during the Cold War has blossomed into a domestic policy alliance, establishing commonalities of security and facilitating significant and increased collaboration on shared problems. This is not an ad-hoc development; there is a distinct identity formation process occurring.

The three areas of cooperation are: law and cyber-crime; immigration, borders, and asylum; and, domestic violent extremism. Data is shared in all of these domains. There are huge concerns with obstructions surrounding encryption, and the most prominent challenges for the future of Five Eyes lie in counter radicalisation, pursuit/detection, and public private cooperation. At a ministerial meeting between the five countries in February 2016 the question was asked: 'could we or should we collaborate more in counter terrorism and cyber?'

This security collaboration is a uniquely special and trusted relationship – other countries are not invited in. Ireland – an obvious candidate – is only invited into one tiny aspect. They are hugely secretive but increasingly they are generating a consensus over major policy discourses. There are explicit invocations, not just about the five countries, aiming to promote international standards among foreign partners. They are dominant operationally and they are looking to dominate public policy. They possess an unparalleled cyber intelligence system and will try to converge other countries' approaches.

Internet forensics as a tool in response to cyber fronts

Dr Kamil Yilmaz and **Dr Murat Gunestas**, General Directorate of Security, Turkey

This paper focused on so-called 'cyber fronts'. Cyber front groups have similar organisational features to terrorist and/or revolutionary groups and provide support for such organisations. Yilmaz and Gunestas explained that, since most cybercriminal groups that support terrorist organizations cannot perform attacks that could cause death or devastation, they define such groups as cyber fronts of terrorist groups rather than as cyberterrorists. While cyber front groups may sometimes be strictly bound to a conventional terrorist group, or to a single branch of an organisation, some are not necessarily bound to a specific group; instead, they provide support for many of them. The speakers introduced *CMG-Team* (cyber-median guerrillas), linked with the PKK, as an example for the former, and also referred to *RedHack*, a cybercriminal group that supports all forms of revolutionary groups in Turkey.

CMG -Team's primary responsibility is to protect official PKK sites and support the media branch. They are not responsible for further development and, interestingly, their personal data security is priority number one, ahead of their other activities.

RedHack is its own beast, unbound to any other organisation. In their statute they state that illegal resources dominate their income. Certain measures are in place for members to follow to gain entry to private conversations. They use IRC as a communication channel rather than forums, and are known for their opportunistic nature. For example, when TTNET went down for two hours due to a technical fault, *RedHack* were quick to claim responsibility.

Yilmaz and Gunestas explained that Internet Forensics is a vital phase in today's investigations into cyber fronts. It offers the potential to demystify anonymity – one of the most powerful dynamics of cyber space. It is both possible and necessary to cluster anonymous accounts (they have multiple redundant and substitute accounts). It is impossible to follow the anonymous users without grouping their accounts. Constant monitoring, in addition to this, eventually reveals inconsistencies; for some reason the stepping stone might fail for sudden cases, thus revealing the user's IP address or other aspects of their identities. It is also possible to group several accounts that are emanating from the same server, even if it is a stepping stone. There are numerous ways of collecting intelligence from the web. Little considered are the intentions and actions of rival groups. Politically motivated or otherwise, there are always other groups who will share information about their enemies expressly for the purposes of this being picked up by authorities.

In summary, Internet forensics is a powerful tool in two ways: for constantly collecting data; and, for processing this big data very fast, in real time when possible.

Using social network analysis for the study of public reactions to terrorist events

Daniel Grinnell, Cardiff University

Grinnell's presentation explained how social network analysis may be used to look at the impact social media users have on public discourse after a significant event, in this case after a terror attack. The work was informed by the analysis of empirical data deriving from a technique for the rapid measurement of the proportional impact that individual accounts and the ideological stance to which they subscribe are having on public discourse.

The purpose of the work is to give governments, law enforcement, and security agencies an extra tool in understanding how segmentation, polarisation and generational conflict can play out after a terrorist attack. After the Charlie Hebdo attacks a similar attack was considered 'inevitable' by British authorities. Understanding how these events are collectively processed by the public is a beneficial domain of research, in particular given the potential for these events to spawn conflict and collective action that undermines community resilience.

Law enforcement and intelligence agencies are largely focused on understanding the situation at hand through the establishment of actionable intelligence surrounding the initial event, rather than gauging the community impacts which may result from it. The consequences still play out within society, but the authorities largely move on. In this regard the work seeks to answer three questions:

- Can technological solutions assist in post-event impact detection and analysis 'at pace'?
- Can the most important 'thought leaders' that fuel these post-event impacts and their ideological stance be readily identified?
- What are the policy and operational implications of implementing this sort of analysis within post-event police, security, and government bodies?

Grinnell explained that open source media analysis can allow for the quantification of the impact individual voices and their ideological stance can play in the organisation of extremist post-event collective action. These individuals and their messages directly shape the impact and longer term consequences of the initial event. Conversely it shouldn't be ignored that it is possible for police, security, and government bodies to participate in this messaging and impact the direction that public discourse is taking. This could potentially result in the prevention or diminution of the likelihood of violence, if done appropriately and correctly, through advocating de-escalation via community respected channels.

Recommendations

1. The workshop highlighted the importance of learning from history, from other cultures, from other disciplines and from other research contexts. The value of academic collaboration with non-academic practitioners and policymakers was also emphasised, including the co-creation of research projects and new forms of partnership working. **To fully realise the potential benefits of such partnership, more innovative and more integrated opportunities should be developed to engage academia (including postgraduate research students) at the international level, to feed into policy development, law making, and guidance.** This should include an active commitment to academic freedom and efforts to ensure that academics are able to access, collect, analyse and store data in a secure and ethical manner.

2. Successful multi-agency partnership requires effective communication and inter-partner trust. **A variety of confidence-building measures, that will help to define frameworks of collaboration, intervention and response, should therefore be deployed.** These might include: regional (ASEAN Regional Forum (ARF), EU, AU, OAS, etc.) or track 1.5 table-top exercises integrating stakeholders from the private sector, academia, civil society, NGOs, legal departments, communications departments, etc., to run through 'live' case studies on how to respond to online content; developing and making publicly available a 'cyber game' and database of scenarios that can be used to understand the impacts of interventions and inform policy development; providing a space or collaborative forum where these initiatives, guidelines, scenarios, recommendations, etc., can be accessed by the actors, to stimulate dialogue and engagement; and, providing the public and private sectors with access to, and information on, emerging guidance on how to balance human rights, security and commercial interests in situations involving terrorist use of ICT and the internet, and to engage civil society in the process. Collaboration with the on-going projects on these issues might be a first step in this direction.

3. It is dangerous to conflate the activities of hackers/hacktivists and those of (cyber)terrorists. The former are distinct from the latter, in terms of both their motivations and the impact of their actions. The expertise of this particular community should not simply be ignored; it would be prudent to ensure that flaws which are discovered by hackers/hacktivists are resolved. **To this end, a safe space should be provided for hackers/hacktivists to be able to responsibly report flaws they have discovered in the course of potentially criminal activity perpetrated without malicious intent.**

4. The definitions of terrorism precursor offences must strike an appropriate balance between, on the one hand, the importance of preventing planned acts of terrorism and, on the other hand, ensuring that these offences respect fundamental values and do not over-reach. **Accordingly, the definitions of terrorism precursor offences should be carefully circumscribed, in particular, by requiring proof that the alleged offender had formed an intention to assist, encourage or facilitate terrorism-related activity.**

5. NATO operations have second order effects which may contribute to an environment in which the risk of radicalisation is exacerbated. **Pre-deployment training delivered by NATO member states and partners should be developed in accordance with standards and objectives that nurture cultural awareness in order to mitigate this risk.**

6. An over-emphasis on the suppression of online terrorist propaganda should be avoided, since attempts to suppress such content are beset with practical difficulties and challenges. **It is therefore important that credible and authentic alternative narratives are developed and delivered, and that these narratives are evidence-based and matched by practical action in order not to widen the say-do gap.**

7. Once credible, authentic alternative narratives have been developed, it is vital that these are easily discoverable. **The norms that tech or social media companies and Internet Service Providers develop to govern online content should promote the visibility of alternative narratives.** Recent initiatives aimed at ensuring that those searching for extremist materials online also find alternative narratives are to be welcomed.

8. In terms of terrorist finance, pre-paid cards are an important existing vulnerability. At present an individual can have up to US$2500 with minimal validation of their identity, which is enough to plan, coordinate and perpetrate a terrorist attack. **A higher level of identity authentication should be required to purchase a prepaid card.**

9. More generally, it is important to recognise that financial donations have significant intelligence value. **Financial Intelligence Units (FIUs) should track such transactions in order to disrupt plots and identify individuals involved in terrorist financing.** Doing so will require a willingness to cooperate across borders and share information.

10. The workshop recognised the value of some surveillance activities in protecting national security, but also the harmful effect that misinformation and inappropriate responses have on public perceptions. The workshop therefore stressed that **state surveillance activities undertaken to counter terrorist threats should be accompanied by adequate legal standards and effective guarantees against arbitrariness and the risks of abuse in order to fully respect human rights and individual freedoms.** They must respect the principles of necessity and proportionality and be combined with adequate and independent oversight mechanisms.

Appendix: List of Delegates

Lauri Aasmann (NATO CCD-COE)

Dr Hayrettin Bahşi (Tallinn University of Technology; founding Director, Cyber Security Institute of Turkey)

Dr Karine Bannelier (Université Grenoble-Alpes)

Dr Jamal Barnes (Edith Cowan University)

Burke Basaranel (Swansea University)

Elena Beganu (NATO HQ Counter Terrorism Section)

Sergei Boeke (Leiden University)

Francesca Bosco (UNICRI)

Maj. Giovanni Bottazzi (Head of Network Security, Italian Carabinieri; University of Rome "Tor Vergata")

Prof Roger Bradbury (Australian National University)

Dr Madeline Carr (Cardiff University)

Prof Theodore Christakis (Université Grenoble-Alpes, Institut Universitaire de France)

Dr Maura Conway (Dublin City University)

Joseph Dillon (Dublin City University)

James Fitzgerald (Dublin City University)

Richard Frank (Simon Fraser University)

Bethany Gaines (Swansea University)

Angela Gendron (Carleton University)

Dr Paul Gill (UCL)

Daniel Grinnell (Cardiff University)

Dr Murat Gunestas (General Directorate of Security, Turkey)

Adam Hadley (ICT4Peace)

Sofian Hamiti (Accenture)

Dr Keiran Hardy (Griffith University)

Dr Gokhan Ikitemur (Turkish Ministry of Internal Affairs)

Dr Haroro Ingram (Australian National University)

Dr Lee Jarvis (University of East Anglia)

Dr Camino Kavanagh (King's College London)

Moinuddin Khawaja (Dublin City University)

Loni Lee (Swansea University)

Dr Tim Legrand (Australian National University)

Orla Lehane (Dublin City University)

Sean Looney (Dublin City University)

Prof Nuria Lorenzo-Dus (Swansea University)

Prof Stuart Macdonald (Swansea University)

David Mair (Swansea University)

Chris Marshall (Swansea University)

Anthony McCoy (Accenture)

Lisa McInerney (Dublin City University))

Ltn. Col. Gianluigi Me (Deputy Head of ICT Security Department, Italian Carabinieri; LUISS Guido Carli University)

Dr Holger Nitsch (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research, Germany)

Dr Lella Nouri-Bennett (Swansea University)

Leona O'Reilly (Police Force of Ireland)

Katerina Pitsoli (Swansea University; Université Grenoble-Alpes))

Kristiina Raidla-Puhm (NATO CCD-COE)

Lucy Ray (Dublin City University)

Dr Alastair Reed (Leiden University)

Adam Ridley (Swansea University)

Wolfgang Röhrig (Programme Manager Cyber Defence, European Defence Agency)

Ryan Scrivens (Simon Fraser University)

Paul Shorte (Aide de Camp to the United Nations Head of Mission and Force Commander in Lebanon)

Leonie Tanczer (Queen's University Belfast)

Unal Tatar (Old Dominion University; former co-director, Informatics Policies Commission, Turkish Chamber of Computer Engineers)

Lorena Trinberg (NATO CCD-COE)

Dr Theo Tryfonas (University of Bristol)

Dr Gunnar J. Weimann (independent researcher)

David Wells (former Intelligence Officer at GCHQ, the Australian Signals Directorate and the Australian Crime Commission)

Dr Andrew Whiting (Birmingham City University)

Dr Kamil Yilmaz (General Directorate of Security, Sivas Police Department, Turkey)

Faisal Zaman (Accenture)

Contact Details

ctproject@swansea.ac.uk

www.cyberterrorism-project.org

www.facebook.com/CyberterrorismProject

@CTP_Swansea