TACKLING CYBER CRIME AND CYBER TERRORISM THROUGH A METHODOLOGICAL APPROACH

All Western governments are now searching for ways in which to ensure their cyber national security. To maximise the vast economic and social opportunities that cyberspace has to offer, the British government has transformed its approach to cyber security, setting out a new vision towards 2015 in its cyber strategy: The UK Cyber Security Strategy: protecting and promoting the UK in a digital world. The new strategy now serves to increase all Law Enforcement Agency cyber-related efforts that contribute to its four primary strategic objectives shown in Figure 1.

Figure1: The UK Cyber Security Strategy: protecting and promoting the UK in a digital world

Tackling cyber crime

The emphasis from central government to tackle cyber security as a priority has served to push the investigation of cyber crime to the fore. As a direct result, all UK police forces, as directed by the Association of Chief Police Officers (ACPO), contribute to the UK's Cyber Security Strategy by carrying forward an E-Crime initiative established by ACPO which provides the strategic foundation and direction to ensure that all police forces remain alert to cyber crime activities. Being alert to cyber crime activity in reality means that any suspected online criminality or activity – no matter how small – is reported by the public and the business

sector and recorded. This policing initiative continues to be embedded within the very operating culture of policing practices at all levels of policing and all police officers, whether front line responders, detectives of the Criminal Investigation Departments based at local policing divisions or regional units, all have a responsibility to contribute towards achieving the aim of the national ACPO E-Crime initiative.
Local police forces contribute to the broader cyber crime efforts of the new National Crime Agency (NCA), a powerful body of operational crime fighters who have a clear focus on public protection with a federal approach. The NCA mission shall include tackling organized crime, strengthening borders, fighting fraud and cyber crime, and protecting children and young people. The creation of the NCA marks a significant shift in the UK's approach to tackling serious, organized, and complex crime, with an emphasis on greater collaboration across the whole law enforcement landscape in which all local police forces play a strategic role. Local police forces have been encouraged to develop an effective two-way information sharing relationship with the NCA, to ensure they engage fully in its four operating commands which include the Economic Crime Command (ECC), providing an innovative and improved capability to deal with fraud and financial crimes, including those carried out by organized criminals, and the Child Exploitation and Online Protection Centre (CEOP), which shall work with industry, government, children's charities and law enforcement to protect children from sexual abuse and to bring offenders to account. Both of these primary arms of the NCA shall work to significantly reduce the cyber-based risks to citizens and protect the broader security of the nation and have direct links to the work of local policing. While local police forces tackle cyber-related crime at a local, regional and national level, they are no strangers to tackling more severe threats to their nation's security arising from cyber terrorism and the terrorist use of the internet.

Responding to cyber terrorism

When UK counter-terrorism police officers raided a flat in West London in October 2005, they arrested a young man, Younes Tsouli. The significance of this arrest was not immediately clear but investigations soon revealed that the Moroccan born Tsouli was the world's most wanted 'cyber-terrorist'. In his activities Tsouli adopted the user name 'Irhabi 007', Irhabi meaning 'terrorist' in Arabic, and his activities grew from posting advice on the internet on how to hack into mainframe computer systems, to assisting those in planning terrorist attacks. Tsouli trawled the internet searching for home movies in the theatres made by US soldiers concerning conflict in Iraq and Afghanistan that would reveal the inside layout of US military bases. Over time these small pieces of information were collated and passed to those planning attacks against armed forces bases. This virtual hostile reconnaissance provided insider data illustrating how it was no longer necessary for terrorists to conduct physical reconnaissance if relevant information could be captured and meticulously pieced together from the internet.
Police investigations subsequently revealed that Tsouli had 2.5million € worth of fraudulent transactions passing through his accounts which he used to support and finance terrorist activity. Pleading guilty to charges of incitement to commit acts of terrorism, Tsouli received a sixteen-year custodial sentence to be served at Belmarsh High Security Prison in London where, perhaps unsurprisingly, he has been denied access to the internet. The then National Coordinator of Terrorist Investigations, Deputy Assistant Commissioner Peter Clarke, said that Tsouli: "Provided a link to core al Qa'ida, to the heart of al Qa'ida and the wider network that he was linking into through the internet", going on to say: "what it did shows us was the extent to which they could conduct operational planning on the internet. It was the first virtual conspiracy to murder that we had ever seen." The case against Tsouli was the first in the UK which quickly brought about the realization that cyber-terrorism presented a real and present danger to the national security of the UK – a threat that all in authority required a better understanding to develop and deploy effective counter measures.

Terrorist use of the internet

The threat of cyber terrorism continues to dominate the concerns of national security policy makers, but it is the terrorist use of the internet for recruitment and radicalisation that has spurned a home-frown terrorist threat not just in the UK, by across EU Member States and in the United States. During June of 2006, Hammad Munshi, a 16 year old school boy from Dewsbury in Leeds of West Yorkshire, was arrested and charged on suspicion of committing terrorism related offences. Following his arrest searches were conducted at his family home where his wallet was recovered from his bedroom. It was found to contain hand-written dimensions of a sub machine gun, taken from a book entitled Expedient Homemade Firearm. At the time Munshi had excellent information technology skills and had registered and ran his own website on which he sold knives and other extremist material passing on information on how to make Napalm, as well as how to make detonators for Improvised Explosive Devices (IED's).

While the online rhetoric of al Qa'ida cyber recruiters reached the computer in the bedroom of Hammad Munshi in west Yorkshire, WYP officers on this occasion were able to intervene before any critical security risks to citizens were realized, but not all individuals being recruited online would be prevented from carrying out attack would be stopped by UK security forces. On 22 May 2008, Nicky Reilly, aged 22, left his home in Plymouth with a rucksack containing six bottles full of nails and home-made explosives (HME). His target was the Giraffe restaurant in Exeter, a popular place to lunch for shoppers. Reilly, who has Asperger's syndrome and a mental age of 10, was a suicide bomber, recruited on-line in local internet cafes by extremists in chat rooms who had fuelled a hatred of the West. Extremists had created a home-grown terrorist and had directed him to bomb-making websites discussing what his target should be. As Reilly was seated in the restaurant forty-four customers had also sat down to dine. One of the eleven members of staff working that day brought Reilly a drink, he sat for ten minutes before making his way to the lavatory taking his rucksack with him. Once inside a cubicle the device detonated prematurely causing injury to Reilly and damage to the restaurant. No other person was injured in the blast.
A note left at his home revealed the motivation for his actions in which he paid tribute to Osama bin Laden and called on the British and US governments to leave Muslim countries. The note declared that Western states must withdraw their support of Israel and that violence would continue until 'the wrongs have been righted'. Reilly, appearing at court under the name of Mohammed Abdulaziz Rashid Saeed, pleaded guilty to offences of attempted murder and preparing for acts of terrorism. At the Old Bailey on 30 January he was sentenced to life imprisonment. Mr Justice Calvert-Smith said that: "I am quite satisfied that these offences are so serious that only a life sentence is appropriate. This defendant currently represents a significant risk of serious harm to the public." He went on to say that: "The offence of attempted murder is aggravated by the fact that it was long planned, that it had multiple intended victims and was intended to terrorize the population of this country. It was sheer luck or chance that it did not succeed." The defence counsel, Kerim Fraud representing Reilly stated that: "He may comfortably be deemed to be the least cunning person ever to have come before this court for this type of offence."
The threat of cyber terrorism in all of its forms continues to represent a serious risk to the national security of many nations, but other criminals, extremists, agitators and states themselves have also come to understand the unique potential of the internet, presenting a complex malaise of new cyber-based threats to Western democracies and their citizens. Amongst the many challenges arising from the phenomenon of cyber-based threats and security hazards, remains the urgent need to assess and critically evaluate cyber crimes to identify modes of operation.

Proposed evaluation framework

In order to formally analyse Cyber Crime case studies, such as the ones stated, we propose a model framework for the critical evaluation of cyber crimes based on Strategic Intelligence Management (SIM), the key terms of which include:

- Knowledge Management (KM): "A process of creating a value added Learning Processes (i.e. knowledge) so that knowledge becomes the strategic resource of a law enforcement agency with measurable and quantifiable value in successfully combating a crime or act of terrorism."
- Taxonomic categorisation of KM processes: Gathering, Representing, Organising/Visualising, Contributing, Distributing, Collaborating and Refining.
- Strategic Intelligence Management (SIM): "A term that reflects an assessable framework for a complex matrix of individual or collective mental constructs (thoughts, visions, ideas, insights, learning processes, experiences, goals, expertise, values, perceptions, and expectations) held by individuals, that provides specific guidance for specific actions in pursuit of particular ends. This is undertaken by utilising knowledge within LEAs extended value systems (location, communication platforms, social media, legal requirements, jurisdiction, political and social constrains).
- SIM Formulation: "A pragmatic, action-oriented and result driven process of transforming LEA knowledge use from current status to the desired status based on combined Intelligence and knowledge life cycle which include the processes of collection, analysis, creation, transformation, collaboration, visualisation, storage, evaluation, refinement and assessment."

Proposed model

The formulation of SIM requires a methodological approach. Our approach is based on a review of a number of publicly available intelligence models (e.g. UK NIM, EU IMM) and earlier research by Tolavanen (1998) and

Akhgar (2003). In this context of 'method engineering' we have used a Conceptual Template for the Construction of a Methodology (CTCM) in order to identify and elaborate the core methodological components needed for SIM. CTCM core elements are illustrated in Figure 2.

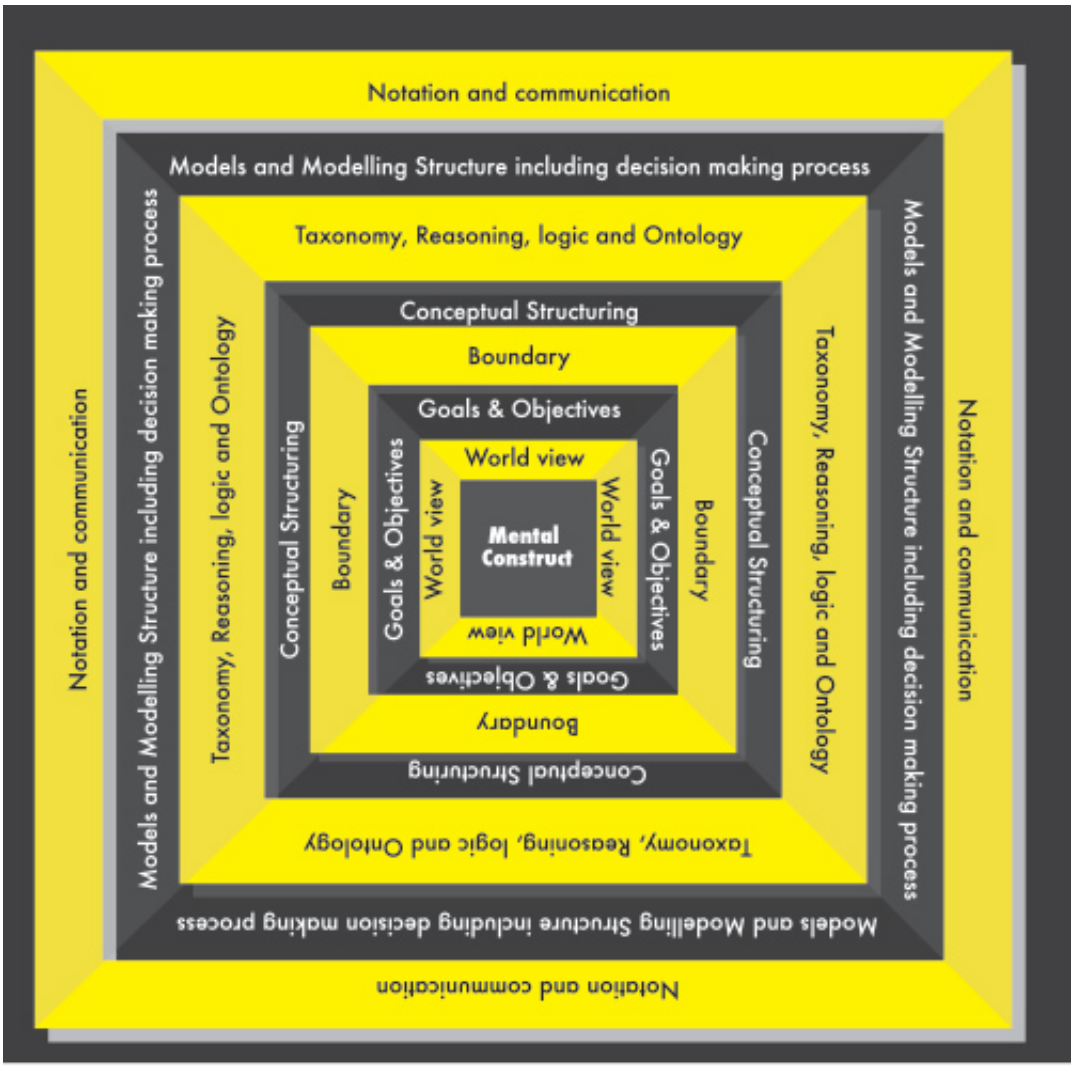

Figure2: A conceptual template for construction of a methodology

Knowledge Management (KM): "A process of creating a value added Learning Processes (i.e. knowledge) so that knowledge becomes the strategic resource of a law enforcement agency with measurable and quantifiable value in successfully combating a crime or act of terrorism."
Taxonomic categorisation of KM processes: Gathering, Representing, Organising/Visualising, Contributing, Distributing, Collaborating and Refining.
Strategic Intelligence Management (SIM): "A term that reflects an assessable framework for a complex matrix of individual or collective mental constructs (thoughts, visions, ideas, insights, learning processes, experiences, goals, expertise, values, perceptions, and expectations) held by individuals, that provides specific guidance for specific actions in pursuit of particular ends. This is undertaken by utilising knowledge within LEAs extended value systems (location, communication platforms, social media, legal requirements, jurisdiction, political and social constrains).
SIM Formulation: "A pragmatic, action-oriented and result driven process of transforming LEA knowledge use

from current status to the desired status based on combined Intelligence and knowledge life cycle which include the processes of collection, analysis, creation, transformation, collaboration, visualisation, storage, evaluation, refinement and assessment."
According to the CTCM (Figure 1) a methodology is based on a number of problem frames (Jackson, 1995) or layers. The shape [original idea of the shape drive from the research by Tolavanen 1998] of the CTCM emphasises that different layers are neither exclusive nor orthogonal (mutually independent). Each layer complements the others and all are required to construct a methodology. Each layer has two facets: a) a conceptual description; and b) an interface projection.

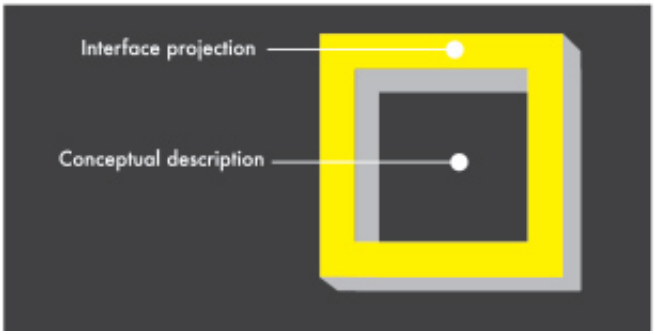

Figure3: CTCM Fragment

The conceptual description is the 'underlying logic' and the interface projection is the instantiation of that logic. In essence the conceptual description represents the absolute view of the object/idea/representation and the interface projection represents the operational view. Below, we describe the core components of this CTCM and how it could be used to construct a methodology for SIM.
Mental Construct Layer
The Mental Construct (MC) layer of the actors within LEAs creating the methodology is the heart of the CTCM. The underlying philosophical paradigm of the methodology derives from this layer. However in law enforcement contexts there is usually more than one person or system (several actors) involved in the development of methodologies. Particularly when dealing with complex and multi-agency operations or investigations such Organised Crime (OC) cases. Hence a question will arise about whose set of mental constructs will be used?
Within the methodology development environment a range of processes will require the production of an overview of the collective set of mental constructs in play for the specific investigation or action. The collective "representation" of the set of methodology creators' mental constructs will form the layer of CTCM, e.g. the UK National Intelligence Model (NIM) and the Europol Serious and Organised Crime Threat Assessment (SOCTA).
The group mental construct (GMC) is a different mental construct than the individual actor MCs; it is rather the representation of dominated factors within each MC. For example different knowledge sets and ethical values from individuals will be projected through the GMC; although there are other elements that might be influential in the formation of the GMC such as political pressure and national security. The projection of the methodology creator(s) mental constructs will be communicated through the description of a World-View. This projection of MC onto the environment creates a semantic representation of the underlying philosophy and the perception of the methodology from methodology creator(s) perspective. It includes all the values, perceptions, understandings and knowledge of the target domain (in this case a criminal or terrorist group). In the context of LEA activity the GMC may force the set of agents working on an investigation or prevention activity (e.g. an investigation team) to address such questions as:

- What are the driving values of the criminal/terrorist group?
- Is there any ideology?
- How much knowledge do we have about the ideology?

- How accurate is our information and knowledge about the ideology?
- Is there any pattern to behaviours? Is there any new crime pattern?
- What are our constraints when dealing with the problem situation?
- How will the end game form?
- What is the financial supply chain?
- What are the consequences of our actions?
- How do we obtain the required intelligence?
- What are the legal issues?
- What are the critical success factors in reducing vulnerability to a terrorist and organised crime attack?
- Are we seeking hard solutions (e.g. technology focused) or soft solutions (e.g. community engagement) for this problem?
- What are our ethical guidelines and codes of conduct?
- What information can we obtain from social media to gain a better understanding about the situation of concern?

Goals and Objectives

The next layer in the CTCM is the goals and objectives layer. Methodologies are not only used to describe the problem domain in the course of an investigation or planning of an operation, but they also should help to improve the "current situation" (before intervention). Before we discuss this layer of the CTCM we have to emphasise that goals and objectives should be based around a clear separation between the uses of the words "goals" and "objectives". Whereby the goals represent the desired outcome in the future – the purpose of the SIM methodology in law enforcement problem solving context – objectives are the points along the way that inform the methodology user if they area on the right track. Objectives identify the critical success factors of an investigation process. This layer of the CTCM is concerned with the contextualisation of the problem situation and its domain. It is used to frame our understanding of a problem. Jackson (1995) refers to this as the "problem frame". It deals with all the aspects of the real world one needs to consider and understand. For example the interrelationship between intelligence components such as the HUMINT and ELINT elements or people linkages directly or otherwise in the course of an investigation. This includes identification of the problem and its type in order to develop goals and objectives. The projection of the aims and objectives of a methodology is communicated to the methodology user through the boundary element of the CTCM. In them methodology construction context it should provide a clear understanding of "what is in" and "what is out" based on the methodology goals and objectives. This is illustrated in figure 3.

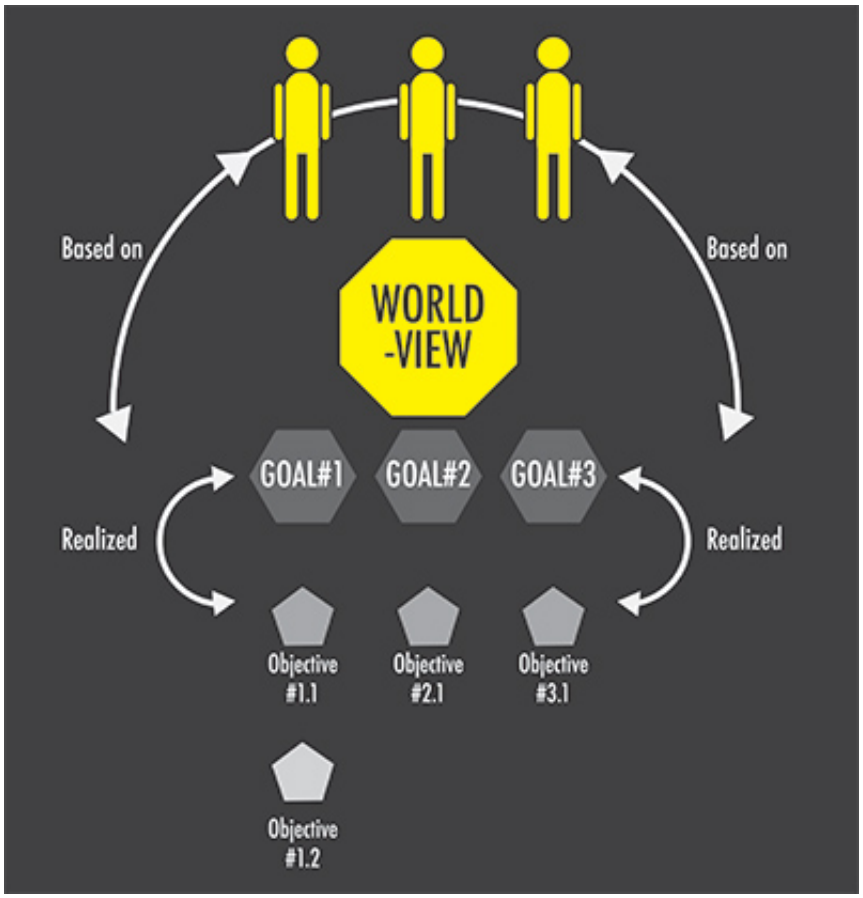

Figure4: Boundary construction for the CTCM

Conceptual Structuring

The next layer of the CTCM is the conceptual structuring. The rationale provided by Jayaratna (1994) asserts that in the context of methodology construction we use structuring [verb] rather than structure [noun] to describe the linkages and organization of concepts. Following this then, during methodology construction it is impossible to simply and statically analyse and completely represent the goals and objectives of the methodology and required actions. It is therefore necessary to restrict attention to a smaller number of concepts and the key meaningful relationship between them. This is particularly important for envisaging the clustering of intelligence captured during an operation and creating a logical and conclusive link between the items of intelligence. The conceptual structuring layer covers procedural guidelines and service descriptions, which describe how the process of achieving the methodology's goals and objectives should be carried out. This is usually based on a national framework or directive such as UK NIM model. The conceptual structuring of a methodology in CTCM is communicated with the methodology user through its taxonomy, reasoning, logic and ontology. This includes the rationale for the steps and stages of the methodology and the user's goals and objectives, which should reflect the methodology's overall goals and objectives as identified in the previous layer. IT should also communicate the key properties (such as the history, dependencies, inherited, events, instantiation, composition and decomposition, states, and emergent, services and roles and responsibilities) needed for planning, tactical understanding and strategic execution of an investigation or an operation (Tolavanen, 1993 and Jayaratna 1994)

Models and the Modelling structure

This layer deals with Models and the Modelling structure. Ontology defined as part of the conceptual structuring layer can be validated and represented globally by using models and taxonomical interaction between models represented through modelling structure. Hence models can be seen as a simplification of

the reality or snap view of what is perceived as reality. The latter also should be implemented for the decision making processes needed within the goals and objectives of the methodology. Jayaratna (1994) stated that models are embedded in the methodologies and their role; type and form help to determine what aspects of reality are captured and understood. In the methodology construction process, models are used to try to gain understanding, and the model's complexity increases as we learn more about the underlying problem domain. For example in a criminal drug trafficking activity the proceeds of the operation may be linked to terrorist activities; therefore our modelling of the drug supply chain may include a clear understanding of a particular terrorist cell. Therefore a combined drug trafficking and terrorism model and modelling structure maybe needed to address the issue. The purpose of creating a model in CTCM is to help law enforcement agents understand, describe, communicate, analyse, or create scenarios with regard to a specific issue of concern.

Notations and Communication

In the CTCM, models and modelling structures are communicated with the user via a notation. How models and modelling structure are defined based on an epistemological view as part of the conceptual structuring, can be discussed and represented only by a notation or set of inter-related notions (see chapter 2 for example of the Odyssey project's Gun Crime analysis notation). The combination of models, modelling structure and notations provides a communication platform in the methodology. The notations can range from formal mathematical representation (e.g. Z) to highly unstructured representation such as rich pictures. Communication standards, both formal and de facto exist in the practice of LEAs. As with any area of professional communication cultural norms and practices have developed within the day-to-day working of LEAs. This is often driven by legal requirements or by formal or de facto standards imported through the use of specific software or the market dominance of specific technologies. For example many crime analysts and investigating officers within LEAs make use of networked graph representations of the links between objects of evidence, people and locations to quickly describe findings or hypotheses. The communication strategies, formats, notations and content used in the CTCM need to fit with the accepted and understood standards known to the methodology creators and users.

A way forward

The proposed framework to evaluate cyber terrorism and cyber crime case studies is an essential part of understanding the components of the threats we encounter. The use of the model will enhance LEA understanding of the challenges we face, helping to develop, design and deliver more effective counter-measures. Both cyber crime and cyber terrorism continue to provide acute security concerns, amplified by the lack of knowledge and understanding of cyber hazards by senior officials and an LEA work force that requires significant investment in training to develop a sophisticated hi-tech investigative doctrine across their full operating landscape. The culture of LEA investigations has quickly changed, organised criminals have dynamically shifted their modes of operating from committing one physical theft or robbery of 1million €, to committing 1 million thefts of 1€ each in cyber space – and LEAs are behind the curve and are now playing catch-up. The most important task for LEAs is to quickly accept an uncomfortable truth: that they cannot tackle cyber threats on their own and moving forward, the most important tool in the armoury of LEAs, shall be their ability and willingness to collaborate with academia and the private sector by sharing important data concerning their operational cyber challenges. The proposed framework to evaluate cyber terrorism and cyber crime case studies provides one such example where academia and operational practitioners bring their expertise to bear in concert one another for the unified goal of preventing cyber crimes ans making online communities safer.

Babak Akhgar
is Professor of Informatics and Director of the Centre of Excellence for Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)
Andrew Staniforth
is Detective Inspector, North East Counter Terrorism Unit, (UK) and Senior Research Fellow, Centre of Excellence for Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC)