Editorial

International symposium on economic crime think tank on "security, intelligence, and law enforcement" Jesus College, Cambridge

On 11 September 2016, exactly 15 years to the day after the events of 9/11, the first meeting of the Security, Intelligence and Law Enforcement (SILE) Think Tank was held at Jesus College, Cambridge, as part of the 34th International Symposium on Economic Crime. In addition to bringing international terrorism to the top of the international security agenda, the events of 9/11 highlighted the crucial role financial intelligence could play in combatting future similar threats. Since 2001, the threat of international terrorism and other security threats such as transnational organised crime have evolved considerably. As the climate of global insecurity deepens, it is more important than ever to gather strength by working closely with our colleagues from all sectors, irrespective of background, rank or seniority to share knowledge and experiences in order that our own organisational responses to these various security threats can be improved.

The concept of the think tanks was developed by Professor Barry Rider, Director of the Symposium, with three main objectives in mind. First, to better capture and enhance the activities of the Symposium; second, to provide continuity between the annual events; and, third, to develop deliverable outputs in terms of papers and think pieces. The aim of the SILE think tank in particular is to examine how intelligence, including financial intelligence, can be better utilised to mitigate security risks associated with terrorism and organised crime. To that aim, as Chair of the think tank, I was greatly privileged to be able to bring together colleagues from a wide variety of professions representing institutions across law enforcement, judiciary, financial institutions, defence and intelligence, the private sector and academia. Furthermore, the panel comprised practitioners from all levels of seniority to enable an in-depth understanding of both strategic and practical/tactical issues. This Special Edition of the *Journal of Financial Crime* has been produced on the basis of discussions which emerged from the first meeting of the SILE think tank.

It is easy to forget that two or three decades ago, organisations were challenged by data paucity. Currently, the reverse is true. As a result of the internet and advancements in related technologies, access to published information and data has led to data deluge, where managing that information has become increasingly challenging but, at the same time, increasingly necessary. For information to be useful, it must be evaluated to sift reliable from unreliable and further analysed to create a product that is fit for purpose – in other words, actionable intelligence.

Good actionable intelligence is needed not only for institutions directly involved in defence and security but also for all sectors wishing not to fall victim to the threats posed by terrorist and criminal organisations. Even within security institutions, there is evidence to suggest that better use of intelligence is necessary, financial intelligence in particular. For example, within policing, far too often time is spent by intelligence officers and staff processing rather than analysing information. The tendency to reject technology as something that is too expensive, or on the basis of the myth that money spent on technology will result in job losses for police officers, is widespread and problematic. But this technology is intended to assist personnel, not to replace them. In addition, technology is becoming far more affordable. In the security environment of the twenty-first century, of which technology and cyberspace are core elements, it is more

Journal of Financial Crime
Vol. 24 No. 3, 2017
pp. 390-392

1359-0790
DOI 10.1108/JFC-02-2017-0014

important than ever to embrace technology, not only to be able to keep up with criminals but also to use the technology against them. To that end, we must learn from other actors in both defence and the private sector to see how cross-sector co-operation can enhance our own organisations. We are stronger together than working in isolation.

It is, therefore, appropriate that the first of the papers addresses this exact issue. Air Commodore Mark Ashwell, RAF (retired), former Director of Intelligence, Capability, Strategy and Policy at the UK Ministry of Defence, describes "The Digital Transformation of Intelligence Analysis". He highlights the potential of digital transformation and innovation opportunities for intelligence analysis, providing insight as to how data and information technologies could be exploited to better understand and counter our adversaries. He explains how automated mining and analysis of data are increasingly providing new insights and understanding in our increasingly interconnected world.

The significance of the networked nature of criminality is also emphasised by Kenneth Murray, the Head of Forensic Accountancy, Police Scotland. In his paper, "Filling Black Holes: Using Business Process Analysis in Criminal Intelligence", Murray highlights the importance of improving the capture of financial intelligence as a means to understanding organised crime and terrorism financing networks. He argues that the ability to understand the distinctive capabilities of criminal funding processes, as well as their networks, is key to filling intelligence gaps. Critically, he warns that inability to adopt these measures will significantly affect the ability of the police to tackle crime and terrorism.

This view is also shared by founder of the Murabin Group Nicholas McTaggart, a former Detective Superintendent who recently retired from the Australian Federal Police after 38 years of service. In his paper "Follow the Money to Achieve Success: Achievable or Aspirational", McTaggart describes the extent to which organised crime and the environment for money laundering and terrorist financing has altered in the past four decades. He argues that money laundering, terrorist financing and economic crime activity are being disguised in the "noise" of business by specialists that have become very adept at their craft and concludes that despite considerable investments made by financial institutions and lawmakers in countering money laundering and terrorist finance, real effectiveness is somewhat doubtful.

Part of this ineffectiveness undoubtedly results from training and education relating to financial crime, including terrorist finance at present not being fit for purpose. David Chave is a serving Financial Investigator (FI) for the South East Regional Organised Crime Unit, aligned to the South East Counter Terrorism Unit, hosted by Thames Valley Police for both functions. In his paper "Proceeds of Crime Training: Bringing it up to date", Chave explains how training currently provided to FIs, and the judiciary is inadequate, directly impacting the ability to prosecute criminals through the Proceeds of Crime Act 2002 and recommends ways in which it can be improved.

Concerns and criticisms of the police are also expressed by David Fitzpatrick, Barrister in England and Wales and Hong Kong, and former Senior Crown Counsel, Hong Kong SAR, People's Republic of China. In his "'Think Piece' on Intelligence, Investigation and Prosecution", Fitzpatrick focuses on fraud and puts forward the view that in England and Wales, the traditional response to fraud, including cyber-enabled fraud, has failed so completely that a new doctrine must be adopted.

A further criticism of the police commonly expressed by the private sector is the lack of feedback on the Suspicious Activity Reports (SARs) which are submitted. This concern is also echoed by Robert Axelrod, Managing Director of Deloitte Transactions

and Business Analytics LLP in the USA. In recognition of the weaknesses of the existing SARs regime, in particular the inability to identify criminal behaviour through systematic feedback, his paper entitled "Criminality and Suspicious Activity Reports" suggests ways in which a reporting institution could improve its own financial intelligence through better capture and analysis of transactional data.

The potential for the private sector to better utilise financial intelligence is also highlighted in Richard Lowe's paper entitled "Anti-Money Laundering: the Need for Intelligence". As former Head of Police within Defence Intelligence, now working for KMPG, Lowe notes that the private sector approach to CTF and AML is based on historic data. He highlights the need for financial institutions in particular to develop financial intelligence which is forward looking and "predictive" and cites examples from Defence Intelligence as models which could be utilised for improvement within the private sector.

In the context of combatting international terrorism and organised crime, a key aim is preventing our adversaries from accessing finance. The purpose of legislation and regulations after all is to attempt to make the environment more challenging for terrorists and criminals to operate in. However, in doing so, it is often easy to overlook the unintended consequences of measures taken to disrupt our adversaries. One example is the existing trend of bank de-risking, whereby concerns regarding to compliance with CTF/AML legislation and regulations have resulted in banks deciding not to manage the risks, but to avoid them altogether. One consequence has been the denial of banking services to legitimate organisations operating in high risk jurisdictions, impacting their ability to deliver aid or provide socio-economic assistance to post-conflict states already vulnerable to crime and terrorism.

It is therefore appropriate that the final paper in this Special Edition is presented by Dr Justine Walker, Director Financial Crime (Sanctions and Bribery) at the British Bankers Association (BBA), who highlights the impact of the unintended consequences of the existing AML/CTF regime on humanitarian organisations operating in conflict and non-conflict environments. In her paper "The Foreign Policy Tool of Sanctions, Conflict and Ensuring Continued Access to Finance", Walker cautions that the foreign policy intention of economic sanctions, when combined with licensing complexity and other risk factors such as terrorist financing, are not achieving their intended goals. She concludes that recalibration of the sanctions architecture is required to address this issue, and that a new equilibrium needs to be created to ensure the ability of international banks to support permissible humanitarian and development payments.

Overall, this Special Edition illustrates a range of measures which could be adopted by both public sector institutions such as the police and private sector institutions to better utilise financial intelligence and intelligence more broadly to combat terrorism and crime. At the same time, thought must be given to the unintended consequences of pursuing those goals to ensure that the CT and regulatory environment does not become so restrictive that it prevents operations by legitimate organisations. In terms of CTF and AML specifically, it is crucial to avoid creating a two-track system, forcing legitimate funds underground where they will be more vulnerable to abuse by terrorist and criminal organisations.

Shima D. Keene
Institute for Statecraft, London, UK