Review of International Studies (2009), 35, 903–915 Copyright © British International Studies Association
doi:10.1017/S0260210509990349

Managing national security and law enforcement intelligence in a globalised world

KEVIN A. O'BRIEN

Abstract. This article argues that there are five major challenges currently facing Western intelligence communities. First – ensuring skills retention for intelligence officers and analysts, while developing knowledgeable managers and customers, all in an increasingly-complex security environment. Second – instituting and inculcating knowledge and expertise in these staff – while addressing an opponent in al-Qaeda which demonstrates increasingly sophisticated use of IT, new media, etc. Third – drawing-in outside expertise from the research and business communities, as is done currently in the US and Canada but in only a very limited manner in the UK. Fourth – overcoming institutional rigidity in dividing the foreign and domestic – alongside rigid sharing and co-operation relationships. Fifth – creating truly collaborative environments that offer genuine socio-cultural incentives to collaboration rather than mere 'IT solutions'.

A paradigmatic shift is occurring in national security intelligence work today. Characterised by a number of seismic shifts in how national security work is conducted, the 21st century security and intelligence landscape has evolved in ways not seen since the consolidation of the modern intelligence environment in 1945. This contrast with the closed, static set of institutions and relationships which developed on this landscape during the Cold War – especially around security and intelligence activities concerned primarily with confronting a monolithic opponent – and which stagnated in the post-Cold War interregnum. Eighteen years after the collapse of the Cold War paradigm, we are witnessing changes which are finally shaking up institutions and relationships from a prolonged Cold War stasis.

The first of these seismic shifts is the almost complete disappearance of distinctions between foreign and domestic threats – and the manner to confront these; the second is the almost total integration of law enforcement, at all levels of governance, into national security work. The former has meant that the traditional divisions of labour, mandate and responsibility noted in the institutions of intelligence have become less relevant as the threat – primarily from transnational terrorism but also from proliferators of weapons of mass destruction, transnational serious organised crime, malicious cyber-actors, and foreign intelligence services (particularly those linked to the first four threats) – has become global. While previous forms of terrorism also operate across borders – for example, Irish Republican, Western neo-Marxist, or Palestinian – the transnational nature of these threats was predicated on their operating largely from specific locations

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

against other locations. By contrast, in the 21st century conflict with militant Islam, the threat is universal – with almost no distinction possible between the 'front' and the 'rear', around terrorist bases or support-networks.

Reflecting on the changes that this has wrought in the intelligence communities of not only the Quadripartite partners – Canada, US, UK, Australia – but also on those in a number of European capitals (such as in France, Denmark, The Netherlands, Sweden and Germany), it is clear that this shift in the threat focus is leading to changes in the institutions of intelligence. This is underlined by the establishment of terrorism / threat analysis centres in many of these countries which use a fusion-based approach to integrating threat intelligence from a variety of sources and producing products for use by all stakeholders in those intelligence communities. It has also led to a shift in the relationships which underpin these institutions – not only domestically but also in terms of the dramatic increase in joint-working between the officers and analysts of each intelligence service with their opposite numbers in partner-countries, on issues concerning countering terrorism and radicalisation towards extremist violence. Indeed, these relationships are not limited to those countries of traditional allies, but increasingly to include non-traditional partners from developing world countries and new democracies – in recognition of the transnational nature of this threat.

All of this is occurring at a time of two other seismic shifts in Western societies: the ongoing march of the Information Age, and the potential generational shifts that will occur with the entry into the workforce (and, therefore, into the intelligence and security communities) of 'Generation-Y'. The first challenge these shifts represent concerns the changing security paradigm facing Western societies overall – and the requirements this generates for members of their security and intelligence communities. Strategically, the intelligence-led actions of such communities are moving from *response* to *prevention*, aiming to develop knowledge supporting interventions at a far earlier stage against malicious activity – especially terrorism. Some of these interventions will be overt, while others will be covert. In the case of the former, this increasingly involves dynamic preventive security measures (human, physical, technical, procedural) around potential targets of terrorism or espionage. While in the case of the latter, this involves aiming for earlier thresholds of detection of terrorists or foreign agents in order to conduct surveillance on and generate further intelligence leads. This reflects directly on the second strategic shift – moving towards a national security approach characterised by a balance between *investigation and prosecution* and *intelligence-led interventions* which may not lead to arrest and prosecution or ejection. This constitutes a notable shift away from the attitude in some Western countries in the first years after 9/11 that we could somehow 'arrest our way out of this'.[1]

Operationally, over the last decade we have witnessed a shift in the preventive security paradigm from *point defence* to more *holistic security frameworks*, which include significant public-private interactions and partnerships. Not all of these

[1] While this may be the case in the US, historically in the UK this was less the case – as one former senior intelligence official noted, 'when dealing with the IRA we only moved to prosecution if there was no other way in which we could disrupt, divert, disinform, etc, while taking-away some of that sense of grievance within the community through significant financial investment in Northern Ireland' – both points which witnessed significant divergences between 2003 and 2008 in the UK. Interview – former security intelligence official, London – January 2009.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

partnerships are comfortable ones – witness the difficulties that the US Information Sharing and Analysis Centers (ISACs) have had since their inception in the late-1990s – but they are perceived as a clear necessity in today's security environment. A significant focus of this interaction has been on the critical national infrastructure, both physical and cyber. This is demonstrated by government outreach activities such as Project GRIFFIN in the City of London, which draws in corporate security staff to supporting law enforcement on local counter-terrorism and civil contingencies concerns. Also, by the Information Assurance Advisory Council, which brings together government departments and leading companies concerned with information assurance and critical information infrastructure protection. There are also numerous initiatives at the local level which aim to enhance these relationships between local law enforcement particularly and business and industry, for example, the NYPD's Operation NEXUS which builds relationships between all business sectors across New York City and the police for counter-terrorism and counter-crime purposes.

These developments also reflect increasing efforts to frustrate terrorist *attack-planning* at an earlier stage, detecting terrorist plotting in and around potential targets – while tying such detection and prevention activities to wider efforts to halt the radicalisation and recruitment of potential terrorists, or the development of other elements (such as bomb-making, logistics, financing, etc) which support terrorist attacks. There are now efforts to detect and disrupt terrorist plots in their planning stage – focused significantly on detecting what is often referred to as 'hostile reconnaissance' or other suspicious activities and behaviours potentially indicative of terrorist intelligence-generating activities – at the earliest point possible. The intention is that more plots will be disrupted more often or better evidence can be generated, through allowing the plotters to develop their planning under covert surveillance, to be used in courts once the individuals have been arrested and charged.

Legislation and the courts – in the UK and other Western countries – has extended the 'threshold of illegality' to the ever-earlier stages of terrorist planning activities, and recent UK terrorism legislation now includes 'acts preparatory to terrorism'. In some recent UK cases – such as Operation CREVICE (those plotting to attack Bluewater Shopping Centre and London nightclubs) or Operation RHYME (the case centring on Dhiren Barot's reconnaissance of potential targets in London, New York and New Jersey in 2004) – the legislation has not only been upheld but has found accommodation (albeit not always comfortably) with human rights parameters. In other cases – such as the ongoing trial of eight alleged terrorist plotters in Toronto, arrested in June 2006 for allegedly plotting to bomb Toronto's financial district and kidnap and decapitate the Prime Minister in Ottawa – it is proving far more difficult to demonstrate concrete malicious intent in court. Despite the fact that Canadian authorities had the plotters under both covert and overt surveillance for at least seven months prior to their arrests and were able to gather significant amounts of evidence for use in the case. Similar problems have emerged in several US court cases recently – such as the 'Liberty City Seven' plot developed in Miami to attack the Sears Tower in Chicago. Here FBI law enforcement infiltrators and covert sources were accused by the courts of taking an aspirational but incapable group forward to the point of developing a full plot that both would never have occurred without that outside influence. Some

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

have asserted that this was actually more the result of such covert infiltrators than those accused. Another example is the alleged plot to attack fuel-pipelines at New York's JFK airport, which also demonstrated a less-than-capable 'plot' hyped-up by government officials.[2]

This has also served to push, more and more, for intelligence to be generated to evidential standards by those in law enforcement and national intelligence pursuing such plotters, as well as for intelligence, such as intercept evidence in the UK, to be used openly in court. The concerns that this is raising amongst government and law enforcement officials – that their methods and practices, as well as potentially sources, will be exposed publicly and used advantageously by adversaries – is a serious matter. Indeed, it is possible that the attempted car-bombing of London's Haymarket district in June 2007 may have leveraged openly-available court expert evidence from the RHYME trial regarding a similar attempt by Barot to use limousines packed with gas-cylinders as part of that plot.[3]

The management of the closely entwined relationship between law enforcement and national intelligence is of the utmost importance here, with increasing levels of joint-working between the two elements at a time when the whole of law enforcement are being pushed increasingly towards intelligence-led activities. This is underlined by the development of co-located regional capacities by both the Security Service and Special Branch structures in the UK.[4] This is the case not only in the UK, but also in the US – where FBI-led Joint Terrorism Task Forces, Terrorism Early-Warning Groups centred on Sheriff Departments in American counties, and a new 'information-led policing' initiative by the LAPD reflect this trend. This is also the case in Canada – where the development of four Integrated National Security Enforcement Teams (INSETs) have demonstrated joint-working across agencies at the municipal levels tied to national counter-terrorism efforts by

[2] See C. Anderson, 'Mistrial in Sears Tower Bomb Plot Trial', AP (13 December 2007), {http://abcnews.go.com/TheLaw/FedCrimes/wireStory?id=3996409}; Rupert Cornwell, 'Tall stories: The plot to topple Chicago's Sears Tower was not all that it seemed', *Independent* (UK), (25 June 2006), {www.independent.co.uk/news/world/americas/tall-stories-the-plot-to-topple-chicagos-sears-tower-was-not-all-that-it-seemed-405399.html}. See also Joanna Walters, 'Three held, one sought for bomb plot at JFK airport', *The Observer*, (3 June 2007), {www.guardian.co.uk/world/2007/jun/03/usa.joannawalters}. More generally concerning the questionable nature of a number of alleged terrorist plots prosecuted in the US since 2001, see Tim Dickinson, 'Truth or Terrorism? The Real Story Behind Five Years of High Alerts', *Rolling Stone*, (7 February 2008), {www.rollingstone.com/politics/story/18056504/truth_or_terrorism_the_real_story_behind_five_years_of_high_alerts}; Brian Doherty, 'Where's the Terror? Post-9/11 prosecutions end with a whimper', Reason.com, 11 September 2006, {www.reason.com/news/show/36832.html}; or Bruce Schneier, 'Portrait of the Modern Terrorist as an Idiot', *Wired*, (14 June 2007), {www.wired.com/politics/security/commentary/securitymatters/2007/06/securitymatters_0614?currentPage=all}.

[3] *R v Barot*, Court Of Appeal (Criminal Division), [2007] EWCA Crim 1119 [Transcript: Wordwave International Ltd (A Merrill Communications Company)] – Hearing-Dates: 3 April, 16 May 2007 (16 May 2007). However, an article in an Indian newspaper – purporting to detail information from Indian investigators following-up on any connection by the Glasgow airport bomber Kafeel Ahmed to the Subcontinent – notes that the failure of the car-bomb was due to the bombers' technical inexperience rather than any other cause: see Praveen Swami, "Glimpses into the mind of suicide bomber: Internet records provide insights into likely cause for failure of three car bombs assembled by Kafeel Ahmed", The Hindu (14 July 2007): {www.hinduonnet.com/2007/07/14/stories/2007071458960100.htm}.

[4] See, for example, Security Service, *Responding to the threat:* {www.mi5.gov.uk/output/Page552.html}; and Association of Chief Police Officers, *POLICE REFORM GREEN PAPER: The Future of Policing* (March 2008), {www.acpo.police.uk/asp/policies/Data/ACPO_submission_re_Green_Paper_20_March_2008_(PUBLIC).pdf} – particularly ch. 4.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

the RCMP and CSIS;[5] and in France – where the amalgamation of the domestic police intelligence agency Direction Centrale des Renseignements Généraux (DCRG) and the security service Direction de la Surveillance du Territoire (DST) represents a similar step in this direction.[6] Such complex joint-working – balanced across all levels of governance, as well as both within and between agencies – in other Western countries is also beginning to reflect such effective approaches in an increasingly-complex security environment.

All these issues are tied to the changing nature of the threat. In those countries with a history of terrorism – such as the UK, France, Spain, Germany, and Italy – the character of terrorism has shifted from by-and-large mono-ethnic, domestically-based, hardened brigades to a multicultural 'nebula' of like-minded individuals driven by the same ideology but who may never have actually met physically. An example of this is the UK's Operation MAZHAR with jihadist plotters drawn from the UK, US, Canada, Sweden, Bosnia and Indonesia.[7] Indeed, the terrorist threat in some countries represents both styles of organisation as co-existing within *Al-Qaeda*-style Jihadist terrorism. For example, both the CREVICE and 21 July 2005 plot would appear to indicate that *Al-Qaeda*'s leadership in Pakistan's Federally Administered Tribal Areas (FATA) maintains a significant degree of direct command and control over some of the Jihadist cells uncovered in the UK since 2001, while other plots and cells may have little, if anything, to do with *Al-Qaeda* core beyond inspiration. From a counter-terrorism perspective, this complex mix of actors and relationships makes it very difficult to judge which individuals or cells uncovered – oft-times tangential to others – should be given priority. MI5 Director-General Jonathan Evans identified approximately 2000 individuals of counter-terrorism concern in November 2007.[8] Such difficult considerations would appear to have informed decisions made by British counter-terrorism officials when Mohammed Siddique Kahn and Shazad Tanweer were identified consorting with members of the CREVICE network, but were determined to be of a lower priority at the time – a decision that was thrown into stark relief on 7 July 2005.[9]

There has also been a significant shift in the targeting-base of current terrorism. Whereas previously, terrorists tended to ascribe to Brian Jenkins' aphorism that they 'want a lot of people watching, not a lot of people dead',[10] contemporary Jihadist terrorism aims for mass casualties and mass catastrophes, almost entirely

[5] See, for example, RCMP, 'Integrated National Security Enforcement Teams (INSET)': {www.rcmp-grc.gc.ca/security/insets_e.htm}.

[6] B. A. Jackson (ed.), *Considering the Creation of a Domestic Intelligence Agency in the United States: Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (RAND, 2009): {www.rand.org/pubs/monographs/2009/RAND_MG805.pdf} – 65.

[7] See, for example, S. Swann, 'Aabid Khan and his global jihad', *BBC News* (18 August 2008), {http://news.bbc.co.uk/1/hi/uk/7549447.stm}; Daniel McGrory, 'British computer whiz-kid exports terror via internet', *The Times Online*, (7 June 2006), {www.timesonline.co.uk/tol/news/uk/crime/article672452.ece}.

[8] Jonathan Evans, *Address to the Society of Editors by the Director General of the Security Service*, 5 (November 2007), {www.mi5.gov.uk/output/Page562.html}.

[9] See P. Taylor, 'Panorama Special: Real Spooks', *BBC Panorama*, (30 April 2007), {http://news.bbc.co.uk/1/hi/programmes/panorama/6476207.stm}.

[10] See B. M. Jenkins, 'International Terrorism: A New Mode of Conflict', in David Carlton and Carlo Schaerf (eds), *International Terrorism and World Security* (London: Croom Helm, 1975), p. 15; see also G. Krikorian, 'Calmly taking terror's measure', *LA Times*, (31 January 2008), {http://articles.latimes.com/2008/jan/31/nation/na-jenkins31}.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

against soft-targets, such as public transport in Western countries – together with their allies and assets in the Developing World. Extending counter-terrorism measures overseas has, therefore, been a focus for security assistance programmes – specifically around law enforcement and military forces – run by Western countries with their allies and partners in both newly-emerging democracies and the Developing World.

Terrorism is not, however, the only growing concern for the UK and other Western security officials. Recent pronouncements by leading security officials in the US (such as the head of the US Counter-intelligence Executive) and the UK (as also noted in the aforementioned speech by Jonathan Evans) that Chinese and Russian espionage is increasingly dramatically highlights one of the current dilemmas. As national security apparati are recast to focus on counter-terrorism and homeland security, the ability of the security services to confront other threats to national security may be degrading. This loss of significant expertise in counter-espionage and counter-intelligence – is matched by the dramatic (over-) burdening of security forces, particularly in the UK, with confronting terrorism. While many assert that terrorism represents the most immediate, tangible threat to the fabric of Western society, the increasing boldness of Russian and Chinese intelligence services in their actions within these societies demands a response from the UK and US security services. This was witnessed by the Litvinenko poisoning case in the UK and the arrests of a number of Chinese intelligence operatives in the US over the last decade. Whether the resources and expertise remain to address this problem is unclear.

Reflecting the above paradigmatic shifts – in both the security environment and the threat – intelligence for countering terrorism and other threats to national security is being reshaped in the UK and other Western countries. At both the national and operational levels, the shift in balance from strategic to tactical intelligence requirements – and from overseas- to domestically-generated intelligence – is the most immediately noticeable. This reflects the rise in significance of the 'very local' in contemporary intelligence, as part of the increased importance and centrality of 'community intelligence' – and the accelerating importance of frontline law enforcement in countering terrorism. It is for this reason that intelligence communities are also emphasising jointery – through such organisations as JTAC in the UK, ITAC in Canada, NCTC in the US, NTAC in Australia, and their Dutch, German, and Swedish counterparts. Operationally, these developments are reflected in the growth of joint working – such as the INSETs in Canada, the Fusion Centers in the US, the regionalisation of the Special Branch, Security Service and SOCA structures in the UK, and similar initiatives in other countries.

Equally, there has been a dramatic refocusing of national analytic attention onto domestic, tactical intelligence development and requirements – conducted by the security agencies, law enforcement and security policing, borders and immigration agencies, local authorities and social-welfare agencies. This is complimented by a focus on the impact of overseas events and developments on Diasporas from within which terrorist activities emerged. As a result, the previous divide between the foreign and domestic intelligence – especially concerning terrorism – has all but disappeared in the networked, globalised world. This, in turn, is having a direct impact on how national security architectures, institutions and mandates – in the

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

UK, US, Canada and Australia – divided up and co-ordinate responsibilities, labour and resources to deal with these threats. Somewhat ironically, this has been paralleled by more traditional measures to counter foreign espionage by Russia and China at a level not seen since the Cold War.

Law enforcement is playing an ever-increasing role in national security work, alongside their traditional role of countering and disrupting crime. In terms of the dramatic up-scaling of law enforcement involvement in national security work, this has seen the traditional police owners of national security work – the Special Branches in the UK, the FBI in the United States, the RCMP in Canada, the Australian Federal Police, the AIVD in The Netherlands or the BFV in Germany – joined by mainstream police. Everyday police officers now have a dual role in maintaining public safety and security while generating intelligence on potential threats emerging from within domestic communities.[11] This is far too often a cause of tension in itself, as police attempt to find the balance between maintaining community cohesion and public safety against the need for community intelligence and intelligence-led interventions in these communities to counter terrorism and radicalisation. All of this has meant a remarkable confluence of frontline policing and national security work of a kind seen since the Second World War.

In the UK, the four Pillars of the Counter-terrorism Strategy (CONTEST) are to PROTECT against, PREVENT and PREPARE for terrorism, and PURSUE terrorists.[12] The role of the police service in supporting CONTEST is fully intertwined with its role in policing the UK against crime and disorder, while maintaining public confidence and community cohesion. In terms of PURSUE, the UK police have the lead in developing prosecutions against those engaging in terrorist activities under existing terrorism legislation, and work with the Security Service to develop the intelligence and evidence necessary to effect this. In terms of PREPARE, the police service support the Civil Contingencies Secretariat in the Cabinet Office to run exercises and develop mitigation strategies against those attacks which succeed. With regard to PROTECT, the role of the National Counter-Terrorism Security Office (NaCTSO) – working closely with the Centre for the Protection of National Infrastructure (CPNI) at the national level – and its Counter-Terrorism Security Advisors (CTSAs) work with local law enforcement to provide advice on potential or real threats to the critical national infrastructure and private industry in the UK.

The area of greatest complexity is PREVENT. In its assessment of the July 2005 attacks, the UK's Intelligence and Security Committee noted the need to develop a 'richer picture' of the communities from where such terrorists emerged.[13] For the police service, this means leveraging and enhancing existing local knowledge of the streets, neighbourhoods and communities which they patrol and interact with daily. At the same time they have to mindful of the fact that (as Sir Robert Peel noted originally in 1829 concerning the original establishment of the

[11] See, for example, the UK's Counter-Terrorism Strategy II (CONTEST-II) and its emphasis on 'Preventing violent extremism and radicalisation' through much greater community engagement: {http://security.homeoffice.gov.uk/counter-terrorism-strategy/}. Similar emphases have also been placed on countering terrorism from – for example – the governments of The Netherlands, the US, and Canada.

[12] See footnote 11.

[13] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, (May 2006), {www.cabinetoffice.gov.uk/~/media/assets/www.cabinetoffice.gov.uk/publications/reports/intelligence/isc_7july_report%20pdf.ashx} – s131.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

Metropolitan Police Service),[14] they do so only with the consent, support and co-operation of the public. In this sense, the success or failure of the ability of the police and security agencies to develop this 'richer picture' is reliant in the extreme on information provided by the public – either openly or through covert human sources – to highlight individuals or behaviours of concern emerging within their community. Without such 'community intelligence', however, the overall counter-terrorism effort will fail. It is Britain's police services which – like their cousins in other Western democracies – are increasingly shouldering the responsibility for pursuing this aspect of national security work, in partnership with national security agencies. These new duties are set against the increased potential for 'community tensions' emerging partly as a result of such activity. As the London Metropolitan Police Authority warned in its 2007 review 'Counter-Terrorism: The London Debate' and as the Home Affairs Select Committee also noted 2005,[15] the role of the police in generating intelligence from within these communities must be finally balanced against the need to ensure such continued public support for the policing of those communities.

All of this has required an ever-closer – and managed – relationship not only between law enforcement and national intelligence, but also the building of new relationships between the intelligence community and non-traditional partners, particularly in local government. The need for so-called 'community intelligence' domestically has meant that those who have the most frequent contacts with many of the communities from within which terrorists emerge are now being brought into the counter-terrorism partnership as never before. Social-welfare workers and agencies – for housing, for benefits, for employment programmes, for youth programmes, etc – are now on the frontline of countering terrorism. It is not always a comfortable position for them to be in, however local law enforcement – in the UK as much as in other countries – is bridging this relationship while doing its best to be sensitive to the needs of the community and those working to support it. This is also leading to emerging tensions – in procedure, in the institutions which confront such threats, and in the relationships within those institutions – between the nature of the threats (which generally manifest themselves at the national or international levels) and the focal-point for interventions to counter these threats (which must generally be local – indeed, very local). In the UK and some other Western countries, this is leading to a rethinking – and some redesign – of the role of law enforcement in countering terrorism domestically, to account for these inherent tensions.

Much of this push for 'community intelligence' also hinges on the need to assess and understand socio-cultural intelligence efforts in increasingly-cosmopolitan and multi-cultural societies. While this has long been the case in North American societies, it is a newer dynamic for law enforcement and intelligence services to deal

[14] Sir Ronnie Flanagan, *The Review of Policing: Interim Report* (2007), {http://police.homeoffice.gov.uk/publications/police-reform/Review_of_Policing_Interim_1.pdf?view=Binary} – 4.

[15] See particularly, 'Executive Summary' (and then throughout), Metropolitan Police Authority, *Counter-Terrorism: The London Debate*, (February 2007), {www.mpa.gov.uk/downloads/committees/mpa/070222-06-appendix01.pdf} – Home Affairs Select Committee, *Terrorism and Community Relations*, (6 April 2005), {www.publications.parliament.uk/pa/cm200405/cmselect/cmhaff/165/16502.htm}. See also Charlie Edwards, *The case for a national security strategy* (Demos, February 2007), {www.demos.co.uk/files/Demos_report_the_case_for_a_national_security_strategy.pdf?1240939425}.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

with in many European states, to varying degrees. The need to – first – have the human capability to develop and capture such socio-cultural intelligence from within diverse communities (both ethnic and religious), and – second – to understand the nuances, dynamics and other finer points around such cross-cultural inputs as part of analysing the results of these intelligence development and collection activities represent the two sides of this challenge.[16] While this is immediately relevant and obvious in contemporary counter-terrorist activities – especially around modern jihadist terrorism – it is equally-relevant to confronting transnational and serious crime, especially where it crosses-over with terrorism, weapons proliferation, or other threats to national security. To achieve this, recruiting initiatives within both the intelligence and law enforcement agencies, and for both employment and covert human-source purposes, has focused increasingly – in Western European countries, as well as Australia – on ethnic-minority communities, linguistic specialists, or those natives who have lived overseas in countries and communities of interest.[17] While this may sound relatively easy – assuming the willingness of new recruits – when considering the recruitment of new employees with these skills and experiences, it has presented challenges to internal security and vetting procedures, given that these characteristics are exactly the ones which present significant challenges to vetting. Nevertheless, such challenges must be overcome, so that the expertise within the intelligence and law enforcement agencies is as cross-culturally representative as the communities that concern them.

A closely-related challenge is the increasing need to be able to understand and assess effectively cross-cultural indicators of suspicious behaviours and related activities. Terrorists – like insurgents and criminals – require information to plan and conduct their operations; the processes by which they generate this information – then process and analyse it into 'intelligence' (whether tactical, operational, or strategic)[18] – generate indicators from their surveillance and reconnaissance activities. As a result, counter-terrorist communities world-wide have made considerable effort to identify and raise awareness (public, corporate, policing) around such behavioural indicators. However, most efforts have tended to either be non-ethnicity or culture specific, as has been the case in the UK and the USA, or concentrate almost entirely on one culture (as has been the case with Israeli efforts in examining the Arab culture). As noted above, in increasingly multicultural societies – and, specifically, where the global jihadist network has made emphatic its efforts to recruit and use terrorists from non-traditional communities, being able to identify suspicious activities, deceptive measures, and equally innocuous behaviours cross-culturally must inform counter terrorist intelligence activities.[19]

[16] This is similar to the approaches being used in theatres of conflict – such as Iraq and Afghanistan – by the US military's Human Terrain System programme: see Noah Shachtman, 'Montgomery McFate: Use Anthropology in Military Planning', *wired Magazine*, 16:10 (22 September 2008), {www.wired.com/politics/law/magazine/16-10/sl_mcfate}.

[17] See, for example, Secret Intelligence Service, 'Careers as a linguist': {www.sis.gov.uk/output/linguist-careers.html}; or Shane Harris, 'Intelligence File Languishing Linguists', *Government Executive*, (1 July 2007), {www.govexec.com/features/0707-01/0707-01adif.htm}.

[18] See K .A. O'Brien, 'Assessing Hostile Reconnaissance and Terrorist Intelligence Activities: The Case for a Counter Strategy', *RUSI Journal*, 153:5 (October 2008), pp. 34–9.

[19] That is, from the native ethnic populations – usually meaning 'white-eyes', as al-Qaeda has referred to them – in Western societies.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

Paradoxically, while public at large is evidently the central player in many of these issues; these are all occurring at a time of significantly-increased public scepticism concerning intelligence. The spate of terrorism trials involving members of Britain's Muslim communities that the UK government has pursued since 2000 has had a difficult impact on such community relations by the police services. This includes anecdotally a reduction in the degree of so-called 'walk-in intelligence' provided to the police and security services by members of these communities[20] – and on the fine balance required around this public support / public scepticism for government anti-terrorist actions. The fact that some court cases have resulted in UK anti-terrorist legislation being overturned; in individuals being found innocent in front of the courts; and even, in some cases, some seemingly overly-harsh sentences imposed on British Muslims convicted versus other Britons' convictions for very similar offences[21] – have all increased public scepticism and, in the case of Britain's Muslim communities, some degree of antipathy and opposition to national security policing activities within their communities. Similar sentiments have emerged in the Muslim communities of Canada, the US, Australia, The Netherlands, France, Belgium, Germany, and other Western countries following anti-terrorist actions by the authorities which were met with scepticism by those communities' members. Some of this scepticism is due to the fact that – in the UK's experience with terrorism – court-cases dealing with alleged terrorist plots today appear to be far more complex when compared with the plots of Irish Republican terrorism a generation ago. This requires a more nuanced understanding by juries (as has been thrown into stark relief by the failures of both the 7/7 and 'airlines plot' juries to reach verdicts initially in each case).[22] It is, therefore, a perpetual struggle by the police service – as the most visible, community-facing aspect of the national security establishment – to ensure that it does everything possible to balance this overarching requirement for community safety and policing by consent against the need to generate further anti-terrorist intelligence leads through programmes such a 'richer picture'.

The change in the 'ownership' of intelligence reflected above is also reflected in another significant shift around the monopoly of intelligence moving from government to private sector ownership. Many large multinational corporations are now

[20] Interview, senior CT intelligence official, London – April 2009.

[21] Witness, for example, the 2007 sentencing of Mohammed Atif Siddique from Scotland – given eight years for possessing terrorist literature – compared with that of Martyn Gilleard from Goole, Humberside – given only three more years for possessing ready-to-use bombs and other weapons to ignite a race-war in Britain – in 2008), see 'Man convicted of terrorism offences', *BBC News*, (17 September 2007), {http://news.bbc.co.uk/1/hi/scotland/tayside_and_central/6997830.stm} and 'Man jailed for terrorism offences', *BBC News*, (23 October 2007), {http://news.bbc.co.uk/1/hi/scotland/tayside_and_central/7056707.stm}; and 'Man jailed over nail bombs plot', *BBC News*, (25 June 2008), {http://news.bbc.co.uk/1/hi/uk/7473060.stm}.

[22] Following a retrial, three of the airlines plotters (Operation OVERT) were found guilty and sentenced to a minimum of 32–40 years in jail (see Haroon Siddique and Vikram Dodd, "Airline bomb plotters jailed for life", Guardian (14 September 2009): {www.guardian.co.uk/uk/2009/sep/14/airline-bomb-plotters-jailed-life}), while the Crown sought a second retrial for the other three members accused of the plot (see Adian Jones, "DPP seeks second retrial of men accused of airline bomb plot", Guardian (12 September 2009): {www.guardian.co.uk/uk/2009/sep/11/airline-bomb-plot-trio-retrial}). In the Operation THESIUS (7/7) plot, all three accused were found not guilty in a second trial (see Rachel Williams, "Muslim men cleared of 7/7 plot but jailed for attending terror camps", Guardian (30 April 2009): {www.guardian.co.uk/uk/2009/apr/30/july-7-london-bombings-trial}) but two were sentenced to seven years for attending overseas terrorist training camps.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

generating and owning far more intelligence of relevance to a broad range of national interests than the government. They are often based globally and enjoy a footprint in many countries where Western intelligence services remain extremely keen to develop enhanced intelligence (for example, with contractors and humanitarian aid NGOs in parts of the world such as Darfur, Lebanon, etc). This is, therefore, not simply a case of private military, security and intelligence companies developing parallel capabilities and capacities to those found in government circles. Instead it is a much wider ownership of intelligence in MNCs and in boutique consultancies (for example, the growth of 'anonymous research', crowd-sourcing and deep-web mining work) who increasingly provide the long-term expertise and experience to Western intelligence services who have 'lost' significant numbers of employees to the private-sector. This is especially true, but by no means exclusively, in the US homeland security and intelligence communities. Equally, this also demands an increase in public-private approaches to both intelligence generation – through enhancements to sharing amongst (crucially) trusted partners – and to the manner in which such intelligence is used to support critical infrastructure protection. Such partnerships have developed in the UK around the Centre for the Protection of National Infrastructure (significantly through its predecessor-agencies the National Infrastructure Co-ordination Centre and the National Security Advisory Centre), but have had less success taking hold in the US around the ISACs (as noted above) and the relationships of many critical infrastructure sectors with the Department of Homeland Security. Alongside this growing need for a public-private approach to intelligence work, the foreign intelligence services and their networks must continue to develop better HUMINT sources in far-flung regions of the world – including the distasteful but necessary interactions with sub-state criminal, despotic and even terrorist elements closer to the target. The days of US Secretary of State Henry Stimson's distaste for intelligence is long past – as one commentator stated, 'terrorists do not play by the Queensbury rules'[23] Much of the above, taking place in the physical world, is now being matched by the dramatically increased role of cyberspace as an operational environment for intelligence activities. The opportunities to develop intelligence – as well as to run intelligence-led operations – through, for example, chat-rooms, cyber-sourcing, or anonymous crowd-sourcing and surveying are all developing the Internet as a new intelligence landscape. This is resulting in the development of techniques and processes for 'cyber-intelligence' which are witnessing the use of real-world intelligence techniques modified for cyberspace, for example, through the use of IP addresses to both build profiles and target individuals. Such intelligence is also contributing increasingly to e-warfare and information operations, deception and counter-intelligence in cyberspace, enhanced approaches to information assurance and critical information infrastructure protection, and – increasingly – activities to counter terrorist C^4ISR activities in cyber-space. In all senses, therefore, the Internet is now an integral part of all intelligence activities – and, therefore, is but a further contributor to the environment and information-overload challenge. Jim Judd, Director of the Canadian

[23] P. O'sullivan, Director-General, Australian Security Intelligence Organisation – quoted in *Legislative Assembly for the ACT: 2006 Week 5 Hansard* (9 May), p. 1345: {www.hansard.act.gov.au/hansard/2006/week05/1345.htm}. See also Porter Goss, 'Text From the Congressional Record', *C-SPAN Congressional Chronicle*, 1999–05-13/11:11:51–11:19:53 – {www.c-spanarchives.org/congress/?q=node/77531&id=8633393}.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

Security Intelligence Service, expressed concern at the 2008 Global Futures Forum conference at what he called the coming 'Information Tsunami'.[24] Moving in parallel is the dangerous belief that mass data crunching and analysis – combined with deep-Web mining – is the solution to current intelligence needs, given the ubiquity of information and communications technologies in our daily lives today. Practitioners in the US, UK and Canada express increasingly-vocal concern that strategic context and understanding are being lost in the 'digital age of analysis'. As one former senior member of the UK's intelligence community noted, 'we used to focus on collecting the relevant intelligence (mostly covertly obtained) rather than simply collecting as much information as possible on a target. Perhaps that's a function of "the enemy you know" against the one we don't really understand at the moment – made all the more challenging by an enemy who does not really have a strategic plan, more just a sense of grievance playing-out operationally.'[25] In this sense, community intelligence – collected against an ever-widening set of requirements and through a wide-range of channels – potentially answers this quandary.

Finally, all of the above activities threaten to further contribute to the imbalance between collection and analysis efforts. It has long been a criticism – indeed, a truism – of intelligence in Western countries (particularly the US with its vast technical intelligence capabilities in SIGINT and IMINT) that collection efforts vastly outweigh the capacity to analyse and assess the data accrued. Anecdotally, this imbalance is increasing exponentially as this 'information tsunami' grows – with analysis required on an ever-widening and – deepening data-set derived from a dramatic increase in community intelligence, from cyberspace, from an expanded set of 'individuals of interest' in contemporary Jihadist networks. Increasingly, this includes individuals on the periphery of investigations who may become radicalised and recruited to become more active in plots and attacks, and from the necessary synergising of overseas and domestic intelligence threads – alongside traditional covertly-obtained intelligence leads and data. The *only* way to confront this challenge is through a dramatic increase in analytic resources and efforts – coupled with significant enhancements to the support given to Analysts in terms of resources, tools, training and professional development.

Accordingly, the final challenge is the training, professional development and retention of a new generation in high-op-tempo environments, especially when hiring criteria remain generally geared towards *roles* and not *skills* (especially cognitive ones when it comes to enhancing analysis). Most Western security agencies are confronting the same challenges in their current workforce. The Director General of MI5, Jonathan Evans, has noted that 54 per cent of the Security Service are now under the age of 40 today. There is a clear requirement for a far more ethnically-broad and experienced workforce. The increasingly sophisticated IT knowledge and usage amongst the younger members of the workforce is not reflected by their older managers may not have the same understandings or appreciations of IT. Similarly, the urge to push new recruits into the operational environment before they have gone through sufficient training and

[24] CSIS, *Remarks by Jim Judd, Director of CSIS, at the Global Futures Forum Conference in Vancouver* (15 April 2008), {www.csis-scrs.gc.ca/nwsrm/spchs/spch15042008-eng.asp}.
[25] Interview – former security intelligence official, London – January 2009.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press

development is intense – especially in those countries, such as the UK, facing a very high threat. Moreover, retaining such individuals once they have developed their capabilities and attained five or more years of experience, are attractive recruits into the private sector – remains a serious challenge to all Western communities, not the least in the US. Knowledge, expertise and insight are crucial elements of today's intelligence officer and analyst – but how can this be ensured given the above pressures and realities?

Perhaps the greatest – and, as yet, unseen – challenge facing the national security establishment in the future will come within. This is constituted by the involvement of Generation-Y in the workplace. This is a generation whose reading, reasoning, information-processing and attention-spans, understandings and appreciations of sources will challenge the ways in which the intelligence business runs. Moreover, we are likely to see, in all likelihood, highlight serious generational differences and disparities between the cognitive outlook of managers and analysts. As the eminent Oxford neuroscientist Susan Greenfield has warned recently, the way in which information and communications technologies are being used by Generation-Y are having a massive and as-yet unassessed impact on the cognitive processes, abilities, and capacities of these individuals, who are now beginning to enter the workforce. The impact is likely to be strongest in knowledge-intensive organisations.[26] Others – such as Simon and Hart – have also recently highlighted the challenges, indeed potential dramatic failings, such changes to the cognitive processing and reasoning functions IT will have on the intelligence world, against the potentially vastly-enhanced capabilities such IT also offers the intelligence environment.[27]

Ultimately, therefore, while the overall aim of intelligence remains constant, its business processes are changing quite dramatically. Against the background of some of the most paradigmatic shifts seen since the establishment of organised, institutionalised intelligence agencies, the government intelligence enterprise of the 21st century will need to evolve at a far more rapid pace than even before, even to maintain its current capabilities. Most Western intelligence communities have recognised these developments, but it remains to be seen whether they are able to adapt effectively and rapidly enough to confront the threats and other national security challenges of this century.

[26] See, for example – J. Cornwell, 'Is technology ruining children?', *The Sunday Times* (27 April 2008), {http://women.timesonline.co.uk/tol/life_and_style/women/families/article3805196.ece}; see also N. Carr, 'Is Google Making Us Stupid?', *The Atlantic Monthly* (July/August 2008), {www.theatlantic.com/doc/200807/google}.

[27] D. Hart and S. Simon, 'Thinking straight and talking straight: Problems of intelligence analysis', *Survival*, 48:1 (March 2006), pp. 35–60, particularly pp. 37–43.

https://doi.org/10.1017/S0260210509990349 Published online by Cambridge University Press