

THE INTERNATIONAL
CENTRE FOR THE STUDY
OF RADICALISATION AND
POLITICAL VIOLENCE



The Future Actions Series

The Changing Security and Intelligence Landscape in the 21st Century

Kevin A. O'Brien, PhD

October 2008

The logo for eden intelligence, featuring the lowercase letters 'e' and 'i' in a blue, sans-serif font. The 'e' is larger and positioned to the left of the 'i'.

eden intelligence

About the *Future Actions Series*

The *Future Actions Series* features informative papers by leading security experts aiming to address some of the key long-term challenges posed by counter-terrorism and counter-radicalisation. Borne out of the 2008 *International Terrorism and Intelligence Conference* on 9-10 June in London, the series responds to the need to look beyond day-to-day threat analysis to identify emerging challenges and develop strategies for addressing them. Each paper focuses on a specific challenge, providing a brief assessment of its nature, how it will evolve, and how to respond to it.

As we have learned, building forward-looking, effective frameworks for approaching counter-terrorism and counter-radicalisation requires intricate coordination among the diplomatic, military, intelligence and law enforcement communities, as well as cooperation between the public and private sectors. Our hope is to advance the strategic dialogue within and between these areas and to provide a valuable reference for policymakers and practitioners.

Future Actions is co-published by *Eden Intelligence* and the *International Centre for the Study of Radicalisation and Political Violence* (ICSR).

Editor

Vanessa Haas
King's College London

Editorial Assistant

Katie Rothman
Project Manager, International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London

Editorial Board

Gavin McNicoll
Director, Eden Intelligence, London

Dr. Peter R. Neumann

Director, International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London

Dr. Magnus Ranstorp

Research Director, Centre for Asymmetric Threat Studies,
Swedish National Defence College

To order hardcopies or contact the editor, please write to mail@icsr.info. All papers in the *Future Actions Series* can be downloaded free of charge at www.icsr.info and www.edenintelligence.com.

About Kevin O'Brien

Dr Kevin A. O'Brien is the Director of Alesia PSI Consultants Ltd, which provides support to government and the critical infrastructure sectors on security matters. He is an Associate of Libra Advisory Group (UK) and a Senior Consultant to Innovative Analytics and Training, LLC (US). He was previously the Deputy Director of RAND Europe's Defence and Security Programme, and Deputy Director of the International Centre for Security Analysis, King's College London.

Summary

National security intelligence work is witnessing a paradigmatic shift. This dramatic transformation is characterized by several factors, including the almost complete disappearance of distinctions between foreign and domestic threats. Another factor is the integration of law enforcement, at all levels of governance, into national security work and the associated tension between maintaining public safety and security while simultaneously attempting to generate intelligence leads.

At the same time, seismic technological and generational shifts are taking place with the rapid development of information technology and the entry of 'Generation-Y' into the workforce of intelligence and security communities. In the context of these intersecting currents, this paper examines ten specific strategic challenges to today's security and intelligence enterprise.

These challenges include: data sharing both between and within national security-related organizations; a shift in balance from national security assessments being fed primarily by overseas intelligence to domestically-generated intelligence; public skepticism concerning intelligence combined with a dramatically increased role of the public in intelligence development; a dramatic rise of intelligence in cyberspace, matched to the increasing role of cyberspace as an operational environment for intelligence activities; and an imbalance between collection and analysis capabilities.

An examination of the evolving nature of the threat combined with dramatic changes in the operating environment exposes weaknesses and inadequacies within the national intelligence community which require urgent attention and reworking in response.

The Changing Security and Intelligence Landscape in the 21st Century

By Kevin O'Brien

A paradigmatic shift is occurring in national security intelligence work today. Characterised by two seismic shifts in how national security work is conducted, the 21st century security and intelligence landscape continues to evolve in ways not seen since the end of the Second World War. Contrasting with the moribund, 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 stagnated in the post-Cold War interregnum, this landscape is witnessing changes which are attempting to shake-up those very institutions and relationships from their continuing Cold War stasis even today, eighteen years after the collapse of the Cold War paradigm.

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 – principally transnational terrorism but also proliferators of weapons of mass destruction, transnational serious organised crime, malicious cyber-actors, and foreign intelligence services – has become almost entirely global, operating as if in a borderless world.

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 Denmark, The Netherlands, Sweden and Germany), it is clear that this transnational shift in the threat is leading to changes in the institutions of intelligence – witness, for example, 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 internationally between services of

different 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 these threats.

In terms of the dramatic upscaling 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 policing in their dual role of maintaining public safety and security while generating intelligence on potential threats emerging from within domestic communities. This is far too often a cause of tension in itself, as police attempt to balance 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 the inevitable and increased involvement of frontline policing – in neighbourhoods and communities, in its relationship with business and industry, in its relationship with local government, and in the institutions of civil society – in national security work in a manner also not seen since the Second World War. When compared against the requirements of each governments' national security strategies – such as the UK Government's CONTEST Strategy – it is clear that frontline policing now plays an extremely significant role in all national security work. As such, the co-ordination and deconfliction of this work with that of government agencies remains a central challenge to these governments.

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'. As such, there are numerous strategic challenges to today's security and intelligence enterprise – ten of which are examined here.

The first challenge 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 of the malicious activity of such threats – especially terrorism. Some of these interventions will be overt, while others will be covert – in the case of the former, this increasingly involves dynamic protective 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 surveil these to both generate further intelligence leads on them and to pre-empt plots and operations. This reflects directly on the second strategic shift – moving from a national security approach characterised by investigation and prosecution to intelligence-led interventions which may not lead to arrest and prosecution or

ejection. For countering terrorism, in many countries this now means a shift from 'locking them up' to 'countering radicalisation and recruitment' as it becomes clear that it will be impossible to 'arrest our way out of this' as was the attitude in some Western countries in the first years after 9/11.

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, practices, and sources will be exposed publicly and exploited by adversaries – is no small concern; 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 Dhiren Barot to use limousines packed with gas-cylinders as part of that plot¹.

The management of the ever-entwining relationship between law enforcement and national intelligence is of the utmost importance here, with increasing levels of joint-working between the two (for example, through the development of regional capacities by both the Security Service and Special Branch structures in the UK)² at a time when law enforcement agencies are being pushed increasingly towards intelligence-led activities. 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 move, and also in Canada, where the development of three Integrated National Security Enforcement Teams (INSETs) have demonstrated joint-working across agencies at the municipal levels tied to national counter-terrorism efforts by the RCMP and CSIS³. Such joint-working – balanced across all levels of governance (local, regional/state/provincial, national/federal), 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.

These relationships have also had an impact on data sharing both between and, indeed, within such organisations. The need to manage the intelligence information – some obtained from human sources, some from covert surveillance and intercept, and some from open sources – within these relationships is being challenged by the need to share such information ever more widely. This spans

-
- 1 *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).
 - 2 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](http://www.acpo.police.uk/asp/policies/Data/ACPO_submission_re_Green_Paper_20_March_2008_(PUBLIC).pdf) – particularly Chapter 4.
 - 3 See, for example, RCMP, "Integrated National Security Enforcement Teams (INSET)": www.rcmp-grc.gc.ca/security/insets_e.htm.

relationships inter-agency, intra-agency, intra-governmentally, and internationally, and has become of paramount importance between law enforcement agencies and national security and intelligence agencies – aiming overall to break-down traditional barriers and reluctance to share, leading ideally to both enhanced early-warning and enhanced processes amongst partners.

Such sharing is occurring both knowingly – when others within your service or other agencies request such intelligence from you – and unknowingly – when others from many agencies have standard access to the intelligence data held by one agency. In the latter case, the need to develop and manage sharing protocols, access-rules, and manipulation and handling guidelines – traditionally governed by ‘need to know’ principles – is being pushed by what in the US is now being referred to as ‘need to share’ drivers; while this is somewhat driven by the assessment of the 9/11 Commission and others that serious shortfalls in ‘connecting the dots’ of intelligence has led to a degradation of intelligence, it is also being driven by a recognition that the culture of the intelligence world – predicated on hoarding intelligence, sometimes for security reasons but other times for power reasons – must change to meet the needs of 21st century national security.

All of 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 (witness, for example, the UK’s Operation MAZHAR with jihadist plotters drawn from the UK, US, Canada, Sweden, Bosnia and Indonesia – all ‘meeting’ and co-ordinating multiple plots through Internet chatrooms)⁴. From a counter-terrorism perspective, this complex mix of actors and relationships makes it very difficult to judge which individuals or cells uncovered should be given priority (for example, from amongst the approximately 2000 individuals of counter-terrorism concern MI5 Director-General Jonathan Evans identified in a November 2007 speech)⁵, and which should be addressed when higher-priority concerns have been dealt with. Such 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

4 See, for example, Steve 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* (June 7, 2006): www.timesonline.co.uk/tol/news/uk/crime/article672452.ece.

5 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.

that was thrown into stark relief on 7 July 2005⁶. At the same time, as Evans warned, Russian, Chinese and Iranian espionage has continued to grow – especially in the case of the first – to levels last seen during the Cold War.

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 recrafted, in a number of significant ways, in the UK and other Western countries. At both the national and operational levels, the shift in balance from strategic to tactical intelligence requirements 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 (in conjunction with the lead role of the security services for developing the intelligence necessary to fulfil this requirement). 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 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.

This has also been reflected in a shift in balance from national security assessments being fed primarily by overseas intelligence to it being fed by domestically-generated intelligence: historically, the overwhelming focus for intelligence analysis had been significantly on overseas, largely strategic or operational intelligence concerns – trying to determine how what is happening or developing ‘over there’ may affect things ‘here’. Law enforcement is having to play an ever-increasing role in such national security work, matching it to their traditional role of countering and disrupting crime – resulting in significant shifts in how police services accept this role. In the UK, the role of the police service in supporting all four Pillars of the Counter-terrorism Strategy (CONTEST) – to PROTECT against, PREVENT and PREPARE for terrorism, and PURSUE terrorists – 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, UK policing 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.

6 See, for example, Steve 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* (June 7, 2006): www.timesonline.co.uk/tol/news/uk/crime/article672452.ece.

In terms of 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.

In terms of PREVENT, the situation is complex. In its assessment of the July 2005 attacks, the UK's Intelligence and Security Committee noted the need to develop a 'rich picture' of the communities from where such terrorists emerged⁷. For the police service, this means leveraging and enhancing existing knowledge of the streets, neighbourhoods and communities which they patrol and interact with daily – never forgetting that (as Sir Robert Peel noted originally in 1829 concerning the original establishment of the Metropolitan Police Service and as was reiterated by Sir Ronnie Flanagan in his 2007 review of UK policing)⁸, 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 their partner security agencies. Such pursuits are matched 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 was noted by the Home Affairs Select Committee in its 2005 assessment 'Terrorism and Community Relations'⁹, 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, while at the same time not engendering or exacerbating inter-community tensions (for example, between long-term residents and new immigrant arrivals in a community, or between the Anglo-Saxon population and a specific ethnic or religious community in Britain's towns and cities).

All of this has required an ever-closer – and managed – relationship not only between law enforcement and national intelligence, but also the building of

7 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.

8 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.

9 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.

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 like 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 occurring at a time of significantly-increased public scepticism concerning intelligence – which is matched, almost paradoxically, against a dramatically increased role of the public in intelligence development. 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 relating by the police services 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 offences¹⁰ – 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 against confronting the plots of Irish Republican terrorism a generation ago, requiring 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 in each case this summer). 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 such a 'richer picture'.

10 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):

Such a 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 – with many large multinational corporations, based globally including 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), now generating and owning far more intelligence of relevance to a broad range of national interests than the government. 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 – as is popularly believed – but a much wider ownership of intelligence in MNCs, boutique consultancies (for example, the growth of 'anonymous research', crowd-sourcing and deep-web mining work); this is especially the case in 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 CPNI (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.

Much of the above, taking place in the physical world, is now being matched by the dramatic rise of intelligence in cyberspace, matched to the increasing 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 intelligence, surveillance and reconnaissance 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 CSIS Director Jim Judd noted, at the 2008 Global Futures Forum conference, around the coming 'Information Tsunami'¹¹. Somewhat dangerously, however, is the resulting belief that mass data crunching and analysis – combined with deep-Web mining – is

the solution to intelligence needs today, given the ubiquity of information and communications technologies (including cyberspace) in most daily lives today; this may be missing the point, given increasingly-vocal concerns expressed in US, UK and Canada that strategic context and understanding are being lost in the 'digital age of analysis'.

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 (including increasingly 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, professional development, and similar) across some of the key points noted above (such as enhancements to public-private or inter-agency sharing).

To meet the above challenges, the final challenge noted here is the training, professional development and retention 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 workforces today: dramatic changes in demographics (for example, Evans has noted that 54% of the Security Service are under the age of 40 today); requirements for a far more ethnically-broad and experienced workforce; increasingly sophisticated IT knowledge and usage amongst the younger members of the workforce (e.g. new media, Web 2.0, collaborative environments, etc.) while their older managers may not have the same understandings or appreciations of IT; similarly, the decreasing age and experience-levels of middle management in the agencies. Similarly, the urge to push new recruits into the operational environment against resource requirements before they have gone through sufficient training and development is high – especially in those countries, such as the UK, facing a very high threat. Finally, retaining such individuals – especially younger recruits – once they have developed their capabilities and, with five or more years of experience, are attractive recruits into the private sector remains an extremely high challenge to all Western communities, not the least of which the US with its 'contractor' culture in the intelligence and homeland security community. Knowledge, expertise and insight

11 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.

are crucial elements of today's intelligence officer and analyst – but how can this be ensured given the above pressures and realities?

In summary, the greatest challenges facing the Western intelligence communities today centre on ensuring skills retention for intelligence officers and analysts, while developing knowledgeable managers and customers – both in an increasingly-complex security environment today; instituting and inculcating knowledge and expertise – including against an opponent in al-Qaeda today which demonstrates increasingly sophisticated use of IT, new media, etc; 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 (for example, through CPNI or JTAC); overcoming institutional rigidity in dividing the foreign and domestic – alongside rigid sharing and co-operation relationships (as is slowly being overcome by initiatives such the Global Futures Partnerships); and creating truly collaborative environments that offer socio-cultural incentives to collaboration – and are not just about 'IT solutions'. Similarly, (re)creating pure intelligence streams in national security policing (as opposed to developing 'intelligence' almost solely for evidential investigations and prosecution) to ensure proper and sufficient use of the raw data generated through national security actions – alongside overcoming the continuing shortfalls in truly appreciating the role that open-source intelligence and information can play in core intelligence development, analysis and targeting activities – both continue to be key shortfalls in institutionalising a truly holistic and integrated approach to national security efforts today.

Perhaps the greatest – and, as yet, unseen – challenge facing the national security establishment in the future will not come from outside, but from within: the involvement of Generation-Y in the workplace. The potential multiplicity of challenges that this may present – in a generation whose reading, reasoning, information-processing and attention-spans, understandings and appreciations of sources, and related aspects – will not only challenge the ways in which the intelligence business runs (including in the cognitive analytic processes of analysts, intelligence officers and police officers), but also, in all likelihood, highlight serious generational differences and disparities between managers' and analysts' cognitive outlook. As the eminent Oxford neuroscientist Susan Greenfield – among others – has warned recently, the way in which information and communications technologies are being used by Generation-Y (and the generation following them) 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 in Western intelligence and government services;¹² 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

12 See – for example – John 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 Nicholas Carr, "Is Google Making Us Stupid?", *The Atlantic Monthly* (July/August 2008): www.theatlantic.com/doc/200807/google.

IT will have on the intelligence world, against the potentially vastly-enhanced capabilities such IT also offers the intelligence environment¹³.

Ultimately, therefore, the business of intelligence is changing – dramatically. Witnessing perhaps some of the most paradigmatic shifts seen since the establishment of organised, institutionalised intelligence agencies and communities on a mass level in the first half of the 20th century, the government intelligence enterprise of the 21st century will need to evolve at a far more rapid pace than even before, in order to stay not only dominant but – in some cases – even current. Most Western intelligence communities have recognised these challenges, but it remains to be seen whether – against both the significance of some of the above challenges and against daily operational demands which leave, in some cases, little room for evolutionary development – they are able to adapt effectively and rapidly enough to confront the threats and other national security challenges of this century.

13 Douglas Hart and Steve Simon, "Thinking straight and talking straight: Problems of intelligence analysis", *Survival* – 48:1 (March 2006): 35–60 – particularly 37-43.

About ICSR

ICSR is a unique partnership of King's College London, the University of Pennsylvania, the Interdisciplinary Center Herzliya (Israel), and the Regional Centre for Conflict Prevention Amman (Jordan). Its aim is to counter the growth of radicalisation and political violence by bringing together knowledge and leadership. For more information, see www.icsr.info

About Eden Intelligence

Eden Intelligence organises small scale, high impact gatherings on counter-terrorism and security related issues in a strictly closed environment encourages debate and sharing of insights. Its goal is to facilitate dialogue and develop collaborative projects amongst the security and counter-terrorism community's leading experts. For more information, see www.edenintelligence.com

www.icsr.info